INTERNAL RULES
FOR THE CONTROL AND PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING OF
IP "INTERCAPITAL MARKETS" AD

I. GENERAL

Art. 1. (1) These Internal Rules (hereinafter referred to as the Rules) are developed on the basis of Art. 101, par. 1 of the Anti-Money Laundering Act (AML) and in connection with the National Risk Assessment adopted on 09.01.2020 under Article 95 of the AML Act.
(2) **IP "INTERCAPITAL MARKETS" AD**, registered in the Commercial Register at the Registry Agency with UIN 131057477 (hereinafter referred to as the "**IP**"), applies the measures provided for in the AML Act, as an investment broker holding license No. RG-03-0204/24.02.2006, issued by the Financial Supervision Commission (FSC) - an obliged person under Article 4, item 8 of the AML Act.

Art. 2. The purpose of these Rules is to ensure the effective performance of the obligations of the IP, in accordance with the AML/CFT Act and the Regulations for the Implementation of the AML/CFT Act *(the AML/CFT Regulations)*, by establishing rules, controls and procedures proportionate to the nature and size of the business activities carried out by the IP to mitigate and effectively manage the risks of money laundering and terrorist financing identified in the money laundering and terrorist financing risk assessments prepared at the supranational, national and IP level.

II. DEFINITIONS

Art. 3. The terms used in these Rules, in addition to those expressly defined below in the Rules, have the following meanings:

"Prominent political figures" means a natural person who performs or has been entrusted with the following important public functions in the Republic of Bulgaria, in another Member State or in a third country:

1. heads of state, heads of government, ministers and deputy or assistant ministers;
2. members of parliaments or other legislative bodies;
3. members of constitutional courts, supreme courts or other higher judicial authorities, whose decisions are not subject to further appeal except in exceptional circumstances;
4. members of the Court of Auditors;
5. members of the governing bodies of central banks
6. ambassadors and diplomatic mission chiefs;
7. senior armed forces officers;
8. members of administrative, management or supervisory bodies of state-owned enterprises and commercial companies with the state as the sole owner;

9. mayors and deputy mayors of municipalities, mayors and deputy mayors of districts and chairpersons of municipal councils;

10. members of the governing bodies of political parties;

11. heads and deputy heads of international organisations, members of governing or supervisory bodies of international organisations or persons performing an equivalent function in such organisations.

"High risk third country" - countries that do not or do not fully apply the international standards in anti-money laundering as defined by the European Commission in Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high risk third countries with strategic weaknesses and referred to in the AML Act.

"High risk jurisdiction" are those jurisdictions identified as high risk on the FATF website: http://www.fatf-gafi.org/countries/#high-risk.

"Group" means a group of undertakings consisting of a parent undertaking, its subsidiaries and legal entities in which the parent undertaking or its subsidiaries have an interest, and undertakings related to each other within the meaning of Article 22 of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Directives 78/660/EEC and 83/349/EEC of the Council.

"Business relationship" is a business, commercial or professional relationship that is related to the provision of Investment Services and/or Ancillary Services by the IP and at the time of contact is established is expected to have an element of continuity.

"IP Activity" means the provision of Investment Services and/or Ancillary Services.

"Other official personal documents" are:

(a) driving licence and documents for residence, pursuant to Art. 1, para. 5, items 2 and 3 of the Bulgarian Identity Documents Act.

(b) registration card, as referred to in Art. 40, para. 1, item 1 of the Law on asylum and refugees, issued to a foreigner seeking protection in the Republic of Bulgaria.

"Other legal entity" means any unincorporated association or any other legal form, regardless of legal personality, which may enter into legal relationships, hold or manage funds and other financial assets or economic resources.

"Member State" means a State that is a member of the European Union or is part of the European Economic Area.

"Investment services" are as follows:

1. receiving and transmitting orders in relation to one or more financial instruments;

2. execution of orders on behalf of clients;

3. transactions on own account in financial instruments;

4. portfolio management;

5. investment advice;

6. underwriting financial instruments and/or offering financial instruments subject to an unconditional and irrevocable obligation to subscribe/acquire the financial instruments for own account;

7. offering for initial sale financial instruments without an unconditional and irrevocable obligation to acquire the financial instruments for own account (placement of financial instruments);

8. organisation of Multilateral Trading Facility;

9. organisation of Organised Trading Facility.

"Ancillary services" are the following services provided by the IP:

1. safekeeping and administration of financial instruments for the account of clients, including custody and related services such as cash and collateral management, with the exception of the centralised maintenance of securities accounts pursuant to Section A, item 2 of the Annex to Regulation (EU) No 909/2014;

2. provision of loans to investors for their transactions in one or more financial instruments, provided that the intermediary providing the loan participates in the transaction;

3. advising companies on capital structure, industrial strategy and related matters, as well as advice and services relating to business transformations and acquisitions;

4. provision of services related to foreign means of payment insofar as they are related to the Investment Services provided;

5. investment research and financial analysis or other forms of general recommendations relating to transactions in financial instruments;

6. underwriting services for financial instruments;

7. Investment services and activities referred to in items 1 to 6 in relation to the underlying instruments of derivative financial instruments, where they are related to the provision of investment and ancillary services.

"Money laundering" is:

1. conversion or transfer of property, with knowledge that such property has been acquired from a criminal offence or from an act of participation in a criminal offence, in order to conceal or disguise the illegal origin of the property or to assist a person who is involved in the commission of such an act in order to avoid the legal consequences of that person's act;

2. concealment or disguise of the nature, source, location, disposition, movement, rights in respect of or ownership of property, with knowledge that such property is derived from a crime or from an act of participation in a crime;

3. acquisition, possession, holding or use of property with knowledge at the time of receipt that such property is derived from a criminal offence or from an act of participation in a criminal offence;

4. participating in any of the acts referred to in paragraphs 1 to 3, associating with a view to committing such an act, attempting to commit such an act, and aiding, abetting, facilitating or counselling the commission of such an act or its concealment.

Money laundering is also present when the activity from which the property was acquired was carried out in another Member State or in a third country and does not fall under the jurisdiction of the Republic of Bulgaria.

"Client" is any natural or legal person or other legal entity that enters into a business relationship with the IP in order to benefit from the Investment and/or Ancillary Services provided by the IP.

"Persons associated with a Prominent Political Figure" means persons who have the following relationships with a Prominent Political Figure:

1. spouses or persons living in a de facto conjugal relationship.
2. first-degree descendants and their spouses or persons with whom the first-degree descendants live in de facto conjugal relationship;
3. first-degree ascendants and their spouses or persons with whom the first-degree ascendants live in de facto conjugal relationship;
4. second-degree relatives and their spouses or persons with whom the second-degree relatives live in de facto conjugal cohabitation;
5. any individual who is known to be the beneficial owner, jointly with a Prominent Political Figure, of a corporation or other legal entity or is otherwise in a close business, professional or other business relationship with a Prominent Political Figure;
6. any natural person who is the sole owner or beneficial owner of a corporation or other legal entity known to have been formed for the benefit of a Prominent Political Figure.

"Credible credit institution" means a credit institution licensed in a Member State of the European Union or a country party to the Agreement on the European Economic Area or a credit institution domiciled in and from a Member State of the Financial Action Task Force on Money Laundering (FATF), of the Asia-Pacific Group against Money Laundering (APG), of the Eurasian Anti-Money Laundering and Countering the Financing of Terrorism Group (EAG) or of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) of the Council of Europe.

"Credible third country" - a third country (i.e. a non-member state) whose legislation contains requirements consistent with the requirements of the AML/CFT Act, taking into account the level of risk of those countries and the implementation of AML/CFT measures consistent with that level, the availability of the full range of such measures consistent with the FATF requirements and their effective implementation.

"Ordinance No. 38" - Ordinance No. 38 of 21.05.2020 on the requirements to the activity of investment brokers of the Financial Supervision Commission.

'Official identity document' means

a) for Bulgarian citizens, identity documents, in accordance with Article 13 of the Law on Bulgarian identity documents:

- ID card;
- passport, diplomatic passport, service passport, seaman's passport, military identity card;
- driving licence.
- identity documents replacing the passport - temporary passport, official open list for crossing the border, temporary passport for final departure from the Republic of Bulgaria.

b) for citizens of the European Union, the European Economic Area and the Swiss Confederation who are not Bulgarian citizens and their family members - an identity card or passport.

c) for foreigners residing in the Republic of Bulgaria, identity documents, according to art. 14, par. 1 of the Bulgarian Identity Documents Act:

- Refugee card;
- Card of a foreigner granted asylum;
- Card of a foreigner with humanitarian status;

- Temporary card of a foreigner;
- Refugee's foreign travel certificate;
- Certificate for travelling abroad of a foreigner granted asylum;
- Certificate for travelling abroad of a foreigner with humanitarian status;
- Certificate for travelling abroad for a person without citizenship;
- Temporary certificate for leaving the Republic of Bulgaria;
- Certificate for a return of a foreigner to the Republic of Bulgaria.

d) for persons who are not Bulgarian citizens or citizens of a Member State of the European Union, the European Economic Area and the Swiss Confederation, and are not family members of a citizen of a Member State of the European Union, the European Economic Area and the Swiss Confederation, including stateless persons - a passport or a travel document in lieu thereof, which has been issued in accordance with the statutory procedure of the country concerned, in which a visa may be lodged and which entitles the foreigner to return to the country of entry, the country of origin or third country; the photo in it allows establishing the identity of its owner, does not contain alterations, deletions, erasures, additions, etc. in the data, no traces of replacement of the photo, stamps are clear, the image of the photo matches the image of the owner and its validity has not expired.

(e) an identity document issued by a foreign competent government authority with a unique document identification number, date of issue and validity, containing a photograph, the person's name, date and place of birth and nationality.

Residency documents and a foreign driving licence are not "official identity documents".

"Related transactions" are those operations and transactions that meet the following conditions:

(a) a series of successive transfers of cash or valuables from or to the same natural person, legal person or other legal entity which are made in connection with a single obligation where each individual transfer is below the statutory threshold but which together meet the criteria for the application of the due diligence measures under the AML Act, or

(b) a series of transfers through different entities referred to in Article 4 of the AML Act which is related to the same obligation, or

(c) other affiliation established in view of the specificity of the operations or transactions based on the application of measures under the AML Act.

"Senior Management Official" means an officer or employee who has sufficient knowledge of the money laundering and terrorist financing risk exposure of the IP and sufficient seniority to make decisions affecting that risk exposure and need not in all cases be an authority or member of a management or representative body of the IP.

"Incidental Transaction" means any transaction or dealing related to the business of the IP which is carried out outside an established business relationship to the extent that the carrying out of such transaction or dealing is permitted by applicable law.

"Third country" is a Non-Member State, i.e. not a member of the European Union and not part of the European Economic Area.

"FATF" is the Financial Action Task Force on Money Laundering, established by a decision of the G7 Heads of State and the President of the European Commission at the G7 Summit held in Paris in 1989.

"Beneficial owner" means the natural person or natural persons who ultimately own or control a legal person or other legal entity, and/or the natural person or natural persons in whose name and/or on whose behalf an operation, transaction or activity is carried out, and who meet at least one of the following conditions:

1. In relation to corporate bodies and other legal entities, the beneficial owner is the person who directly or indirectly owns a sufficient percentage of the shares, interests or voting rights in that body corporate or other legal entity, including by holding bearer shares, or by control through other means, except in the case of a company whose shares are traded on a regulated market which is subject to disclosure requirements in accordance with European Union law or equivalent international standards ensuring an adequate degree of transparency regarding ownership.

An indication of direct ownership exists when an individual(s) owns ***a shareholding of at least 25 per cent of a legal person or other legal entity***.

An indication of indirect ownership exists where ***at least 25 per cent of the shareholding in a legal person or other legal entity is held by a legal person or other legal entity that is controlled by the same natural person or persons, or by multiple legal persons and/or legal entities that are ultimately controlled by the same natural person(s).***

2. With respect to trusts, including trusts, trustee funds and other similar foreign legal entities formed and existing under the laws of jurisdictions permitting such forms of trust ownership, the beneficial owner is:

a) the founder;

(b) the trustee;

(c) the custodian, if any;

(d) the beneficiary or class of beneficiaries, or

(e) the person in whose principal interest the trust is created or managed, where the individual who benefits therefrom is yet to be determined;

(f) any other natural person who ultimately exercises control over the trust through direct or indirect ownership or other means.

3. With respect to foundations and legal forms similar to trusts, the individual or individuals who hold positions equivalent or similar to those listed in item 2.

A beneficial owner is not the natural person or natural persons who are nominee directors, secretaries, shareholders or owners of the capital of a legal person or other legal entity if another beneficial owner has been established.

"Control" means control within the meaning of § 1c of the Additional Provisions of the Commercial Law, as well as any opportunity which, without constituting an indication of direct or indirect ownership, enables the exercise of decisive influence over a legal person or other legal entity in making decisions on the composition of the management and control bodies, the transformation of the legal entity, the termination of its activities and other matters of material importance for its activities.

An indication of "indirect control" is the exercise of ultimate effective control over a legal person or other legal entity through the exercise of rights through third parties, including, but not limited to, conferred by delegation, contract or other transaction, and through other legal forms providing the possibility of exercising decisive influence through third parties.

Where, having exhausted all possible means, a person cannot be identified as the beneficial owner in accordance with, or where there is doubt that the person or persons

identified is not the beneficial owner, the natural person who holds the office of senior management official shall be deemed to be the "beneficial owner".

III. CRITERIA FOR IDENTIFYING SUSPICIOUS OPERATIONS, TRANSACTIONS AND CUSTOMERS

Art. 4. (1) The IP shall use the following non-exhaustive criteria to identify suspicious operations and transactions with clients when providing Investment Services and/or Ancillary Services:

- Larger or unusual transfers of financial instruments and other circumstances giving rise to suspicion that a risk of money laundering and terrorist financing exists.
- Purchase of large packages of financial instruments when the funds invested do not correspond to the information gathered about the client's financial situation
- Payment of large sums that do not correspond to the financial situation of the client
- Purchase and sale of large packages of financial instruments in circumstances judged by the responsible officer to be unusual of the company (assessed on the basis of all circumstances of the case) and giving rise to suspicion that a risk of money laundering and/or terrorist financing exists.
- Payment by cashless means in BGN or foreign currency for the purpose of purchasing financial instruments and a subsequent request to sell what has been acquired and an instruction to transfer the amounts to an account with a different holder and different from the one from which the amounts were originally received.
- Purchase of large packages of financial instruments where the funds for the transaction have been transferred from another financial institution, from an account with an unknown account holder or from an account for which there is reason to suspect its use as a "letterbox".
- A series of unusual purchase and sale transactions of the same financial instruments by different clients over a short period of time, raising suspicions that there is a risk of money laundering and terrorist financing.
- An order to carry out risky transactions (investing in financial instruments), purchase or sale of financial instruments that may result in significant losses for the investor - inability to liquidate the investments or inability to liquidate them without resulting in large losses in price and there are other circumstances giving rise to suspicion of the existence of a risk of money laundering and terrorist financing.
- Frequent purchases of financial instruments by the same client, where the total amount exceeds BGN 1 million for a short period of time, and where there are other circumstances giving rise to suspicion of the existence of a risk of money laundering and terrorist financing.
- A request for transfer of non-cash financial instruments from a personal account to a client sub-account to the investment broker when the client or his/her proxy has not presented a certification document (depository receipt) for financial instruments or there is another circumstance that raises a suspicion of improper legitimation or representation.
- Transfer of funds to another financial institution immediately after their receipt into an account with the IP, where the account with the financial institution does not

belong to the client and/or there are circumstances giving rise to suspicion of the existence of a risk of money laundering and terrorist financing.

- Accumulation of large sums of money in the client account that is legal entity, inconsistent with its turnover, and subsequent transfer to an overseas account, where the circumstances give rise to reasonable suspicion that money laundering or terrorist financing is intended.
- The funds provided for management or deposited to execute orders to buy financial instruments are initially of a minimal amount and subsequently large additional amounts are deposited, followed by frequent withdrawals/repeated placing of orders to sell financial instruments where this raises suspicions that a risk of money laundering and terrorist financing exists.
- The execution by an individual client of a large number of transactions for small amounts, where the total value is significant and this raises suspicions about the existence of money laundering and terrorist financing risks. The funds made available for management by newly established legal persons are in large amounts which are clearly not commensurate with the capabilities of the newly established legal person or its founders.
- Funds are contributed under a management contract or to funds in order to execute purchase orders for financial instruments from a client, a legal entity associated with the activities of an association or foundation whose objectives approximate the demands or claims of a terrorist organization.
- Orders for the sale of financial instruments are placed, with the client willing to transfer the money into several instalments.

(2) The IP shall use the following non-exhaustive criteria to identify suspicious clients when providing Investment Services and/or Ancillary Services:

- The client does not provide sufficient information about the transaction or the information and documents provided contain obvious discrepancies.
- The client refuses to provide identification documents
- The client provides documents when entering into contracts/placing orders that appear to be forged.
- .
- The client does not provide documents of representative authority
- Representatives or proxies of clients present documents of identity and representative authority whose authenticity raises doubts.
- The official identity documents presented by the client lack basic details that fully identify him.
- The client identifies himself with foreign identity documents, the authenticity of which is difficult to verify and there are other circumstances which raise reasonable doubt as to his identity.
- The signature on the identity document does not correspond to the one provided by the client in connection with the transaction.
- The client does not submit or attempts to delay the submission of certain declarations or certificates of good standing and this is not justified by objective reasons.
- The client shows unusual curiosity about the rules for controlling client documents.

- The client's home or work telephone number is disconnected or does not exist.
- The client shall only make all contacts with the IP through a third party who is authorised with all rights to enter into any type of contract/request and there are other circumstances which give rise to a reasonable doubt that no legitimate purpose is being pursued with the services requested.
- The client provides conflicting information about the purpose of trading in financial instruments
- The client provides contradictory information about the origin of the funds he deposits with the investment broker for the purpose of trading in financial instruments
- The client tries to get close to the IP staff by offering money, gifts or services.
- The client is quick to declare that his cash is "clean" and/or has an unusually good knowledge of anti-money laundering and counter-terrorist financing measures.
- The client is accompanied and observed or the operations are carried out in the presence of third parties, which may give rise to reasonable suspicion of pressure or intimidation.
- The client is a person who is known in the media or other sources or is alleged to be engaged in illegal activity.
- The client is a person listed under the Terrorist Financing Prevention Act
- The client shall indicate the address of the third party as his own address.

(3). IP “Intercapital Markets” AD uses higher risk weights in identifying and assessing risks if the client or the beneficial owner of the client is incorporated, domiciled, resident or carrying on its business or profession, or is otherwise connected with, offshore or in countries not applying the FATF Recommendations.

(4). The illicit, unauthorized sources through which terrorist property can be formed and used are the profits and income of various criminal enterprises that benefit terrorist organizations. Some of these are:

- drug production, smuggling and trafficking;
- theft of identity documents for profit;
- cybercrime through credit card fraud, insurance, social security cards and the like;
- theft, adulteration and resale of humanized milks;
- counterfeiting of retail chains, involving consumer items such as branded clothing, jewellery, fashion accessories and household products;
- international cigarette smuggling;
- alternative remittance systems and unlicensed currency transfers.

IV. RISK ASSESSMENT

Art. 5. (1) In order to identify, understand and assess the money laundering and terrorist financing risks in its activities, the IP shall carry out a Risk Assessment pursuant to Article 98 of the AML/CFT Act, taking into account the risk factors associated with its activities, including those relating to clients, countries or geographical areas, products and services offered, operations and transactions carried out and/or delivery mechanisms.

(2) The risk assessment shall be updated at least once every two years, unless the Regulations, the National Risk Assessment referred to in Art. 95, para. 2 of the AML Act ("National Risk Assessment") and the Supranational Risk Assessment and Recommendations of the European Commission under art. 95, para. 2 of the AML Act ("Supranational Risk Assessment"), instructions and recommendations of competent authorities or significant changes in the risk factors associated with the activity require an earlier update.

(3) In preparing and updating the Risk Assessment, the IP shall take into account and reflect the results of the national risk assessment under Art. 95, par. 1 of the AML Act, as well as the results of the supranational risk assessment and the recommendations of the European Commission under Article 95(2) of the AML Act.

(4) The Risk Assessment referred to in this Article shall be updated by the Executive Directors of the IP every two years and also in the following cases:

- a significant change in the products, services and delivery mechanisms provided or used or in client and geographic factors;
- in the event that the State National Security Agency of Republic of Bulgaria or the relevant supervisory authority, in the course of their supervisory activities, finds violations of the AML/CFT Act and the Internal Rules that adversely affect the Company's Risk Assessment;
- the occurrence of other events or factors that could be material to the overall level of risk arising from the Company's activities.

Art. 6. All new and existing active clients of the IP shall be subject to an assessment in terms of money laundering and terrorist financing risk. Client risk assessment shall be an ongoing and continuous process, which shall be carried out by analysing risk factors for each client concerning:

1. The client and the beneficial owner of the client (where applicable)
2. The behaviour of the client
3. Purpose and object of activity for clients legal entities
4. The country or geographical area in which the client or its beneficial owner is established and the associated money laundering and terrorism risk;
5. The products and services offered by the IP and the type of transactions carried out on behalf of the client;
6. The delivery mechanisms used for the products, services and transactions referred to in point 3. The specific practical steps for assessing client risk shall be set out in a risk matrix prepared by the IP.

Art. 7. Transactions with higher risk clients shall be subject to ongoing and extended monitoring.

Art. 8. The entry into and continuation of business relationships with higher risk clients must be approved by the Head of the Specialised AML Service. The approval shall be in the form annexed to these Internal Rules.

(1) In the approval, the identification data of the client as well as the number and type of the concluded contract should be filled in.

(2) The approval shall be retained for a period of five years from the date of termination of the relationship with the client.

Art. 9. The IP shall carry out a risk assessment of a client in the following cases:

- when registering a new client subject to due diligence;
- when updating the data of an existing client;
- in the event of a change in any of the circumstances (related to the risk factors observed by the investment broker) that may affect the valuation of the client;

Art. 10. As a result of the risk assessment, the clients of the IP are classified as:

1. Clients with a high risk profile - enhanced due diligence measures apply.
2. Clients with a medium risk profile - standard due diligence measures apply.
3. Clients with a low risk profile - standard due diligence applies.
4. Clients with an "under surveillance" profile - enhanced due diligence measures are applied. It is applied when it identifies complex or unusually large transactions or operations, those that are carried out under unusual circumstances for the client, and when it identifies a change in other client information that may pose a money laundering risk.

➢ Risk assessment of products, services and delivery mechanisms

Art. 11. (1) All new and existing products, services and transactions offered or carried out by the IP, as well as the delivery mechanisms, shall be subject to an assessment in terms of their impact on the risk of money laundering and terrorist financing.

(2) The risk assessment of new and existing products, services or transactions shall take into account risk factors relating to the degree of transparency of the relevant product, service or transaction; the complexity of the relevant product, service or transaction; the value, size or duration of the relevant product, service or transaction.

(3) The risk assessment of new and existing delivery mechanisms shall take into account risk factors relating to the extent to which the relationship with the client is established and the transactions are conducted directly; the terms under which the transactions or operations are conducted; the extent to which the IP uses intermediaries or agents and the manner in which the relationship with them is settled.

(4) As a result of the Risk Assessment, the products, services or transactions performed by the IP, as well as the delivery mechanisms, are classified as high, low and medium risk.

(5) The risk assessment under this Article shall be carried out by an IP Front Office Officer. The specific practical steps for assessing the risk of a product, service or mechanism shall be set out in a risk matrix and risk assessment methodology prepared by the IP.

(6) The Head of the Specialized Service under the AML verifies the assessments carried out.

Art. 12. Belonging to the lists under Article 4b of the AML/CFT Act

The IP shall refuse to enter into a legal relationship with a client in all cases where it has established that the client or its beneficial owner is a person who is included in the lists referred to in Article 4b of the CFT Act. The lists can be found at the following addresses:

http://www. dans. bg/bg/msip-091209-menu-bul/2015-06-18-13-03-10 https://eeas. europa. eu/headquarters/headquarters-homepage/8442/consolidated_list_sanction_en

V. DUE DILIGENCE MEASURES TO MITIGATE AND MANAGE THE RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING

Art. 13. (1) In order to mitigate and manage the risks of money laundering and terrorist financing, upon entering into a contract with a client in relation to the activity of the IP, the latter shall take measures to mitigate and manage the risks of money laundering and terrorist financing as set out in this Section.

General rules for the application of the measures for due diligence

- The Company, as an obligated person under the AML, performs due diligence on its clients, which includes the following:

1.1. identifying clients and verifying their identity based on documents, data or information obtained from reliable and independent sources;

1.2. identifying the beneficial owner of legal persons and other legal entities and taking appropriate action to verify its identification in a manner that provides a reasonable basis for the Company to assume that the beneficial owner has been identified, including implementing appropriate measures to clarify the ownership and control structure of the client legal entity;

1.3. gathering information and assessing the purpose and nature of the business relationship established or to be established with the client in the cases provided for in these Internal Rules;

1.4. clarification of the origin of the funds in the cases provided for by law;

1.5. ongoing monitoring of the established business relationships and verification of the transactions and operations carried out throughout the duration of these relationships, whether they correspond to the risk profile of the client and to the information gathered during the application of the measures about the client and/or its business, as well as timely updating of the documents, data and information gathered.

Identifying clients and verifying their identity

Art. 14. (1) The identification of clients shall be carried out prior to the establishment of a business relationship, the performance of a casual transaction or the conclusion of a casual transaction.

(2) The Investment Broker may open an account before the verification of the client's identification has been completed under the following cumulative conditions:

1. the account not to be closed until the verification of identification is completed;

2. no transactions or dealings shall be effected by or on behalf of the account holder until the completion of the identification verification, including transfers from the account in the name of and/or on behalf of the account holder.

Identification of client - natural person

Art. 15. (1) The identification of a client (natural person) shall be made by presenting an official identity document and taking a copy thereof.

(2) When identifying individuals, data is collected on:

1) names;
2) date and place of birth;
3) an official personal identification number or other unique element of identification contained in an official identity document which has not expired and which bears a photograph of the natural person;
4) any nationality the person holds;
5) country of residence and address (a PO Box number is not sufficient).

(3) On the basis of the risk assessment, as well as on the basis of the results of the National Risk Assessment, the Company may collect additional data, information and documents under the terms and conditions of these Internal Rules.

(4) Where the official identity document does not contain all the data referred to in paragraph 2 or cannot be ascertained, the missing data shall be collected by requesting other official identity documents or other official identity documents which have not expired and which bear a photograph of the natural person and taking a copy thereof.

(5) The identification of legal representatives, proxies and other natural persons who are identifiable in relation to a client (legal person or other legal entity) shall be carried out by collecting the data according to the procedure for the identification of a client - natural person as set out above.

(6) The information shall be stored in the client file in the manner set out in Section VII. No printout may be made of the data collected if it is signed after it has been collected by the clerk's QES. The documents collected and/or printouts made shall be kept in the client file in the order specified in Section VII.

Identification of clients - legal entities

Art. 16. When identifying legal persons, data shall be collected on:

1) name;
2) legal form;
3) registered address;
4) management addresses;
5) address for correspondence;
6) actual object of the business and the purpose and nature of the business relationship or of the occasional operation or transaction;
7) term of existence;

8) control bodies, management and representation bodies;
9) type and composition of the collective management body;
10) principal place of business.

Art. 17. The identification of a legal person or other legal entity which is a client of the Company shall be carried out in accordance with the provisions of Article 18 et seq. of these Internal Rules.

Art. 18. In cases where a Unique Identification Code (UIC) is indicated for entities registered in the Commercial Register or the Register of Non-Profit Legal Entities at the Registry Agency, as well as in the presence of an official public commercial or company register in the Member State where the legal entity is registered, the identification of legal entities shall be carried out by making a reference to the Commercial Register or the relevant public register on the account of the legal entity and documenting the actions taken to identify the legal entity.

(1) For the Republic of Bulgaria the official public commercial register is https://portal. registryagency. bg/commercial-register;
(2) For the Republic of Poland https://ekrs. ms. gov. pl/web/wyszukiwarka-krs/stronaglowna/index. html

Art. 19. The conditions and procedure for the documentation of the reference made shall be carried out in accordance with the rules of the AML/CFT Regulations, and it shall be possible to establish:

1) the date and time of the reference;
2) the person who made the reference;
3) the last date of update of the legal entity's account in the relevant register;
4) the client data referred to in Article 16;
5) the documents containing the data referred to in Article 16, where they are not visible in the statement but are available in scanned documents in the legal entity's account;
6) creating a report of all identification actions;

Art. 20. The inquiry shall be carried out in a manner that does not allow:

1) changing the sequence of actions taken;
2) unlawful destruction and/or deletion of the reference;
3) unauthorised access, modification or distribution of the reference.

Art. 21. The Board of Directors of the Company shall determine whether the report shall be kept in electronic or paper form and shall adopt additional rules in this regard, if necessary.

Art. 22. In all other cases, the identification of legal persons and other legal entities shall be made by submitting:

- an original or notarised copy of an official extract from the relevant register of current status;
- a certified copy of the Memorandum of Association, the Deed of Incorporation or any other document necessary to establish the data referred to in Article 16;
- a certified copy of the relevant licence, permit or registration certificate (if the activity is subject to licensing or permit).

  Where the documents do not contain the data referred to in Article 16, they shall be collected by submitting other official documents.

Art. 23. The information shall be stored in the client file in the manner specified in Section VII. No printout may be made of the data collected if it is signed after it has been collected by the clerk's QES. The documents collected and/or printouts made shall be kept in the client file in the order specified in Section VII.

Verification of identification

Art. 24. The identification made under this Section shall be verified by one or more of the following means:

(1) Request for additional documents;

(2) Bank references even for the purpose of verifying the identification under par. 1 (Art. 55 AML Act) will not be required from countries that fall under the FATF's prohibition and watch lists. Verification of identification is allowed by requesting documents only from credit institutions from the Republic of Bulgaria, from another Member State or from a bank from a third country under Article 27 of the AML Act.

(3) Confirmation of the identification by another obliged person under Article 4 of the AML/CFT Act (if applicable) or by a person that is required to implement anti-money laundering and anti-terrorist financing measures in another Member State or in a third country whose legislation contains the requirements contained in the AML/CFT Act;

(4) Consultation of public registers, including databases, websites of local and foreign competent state and other authorities, which are publicly accessible and can be used to verify the validity of identity documents and other personal documents collected during the identification;

(5) Establishing a requirement that the first payment under the operation or transaction be made through an account opened in the name of the customer with a credit institution from the Republic of Bulgaria, from another Member State or from a bank from a third country under Article 27 of the AML Act;

(6) Re-request of the documents presented at the time of identification and verification of any change in identification data - when verifying identification in the course of an established business relationship, where the identification was made at the time of entering into such a relationship;

(7) Making inquiries in publicly available local and foreign official commercial, company, corporate and other registers.

Art. 25. If by the above means the identification made cannot be verified, the following means may be applied:

1) use of technical means to verify the authenticity of the documents submitted;

2) any other means that gives the Company reason to believe that the identification of the client is reliable.

Art.26. The Head of the Specialised Office under Article 106 of the AML Act shall issue and maintain up-to-date prescriptions and clarifications on which methods to apply in the cases of clients from certain countries, as well as on the specific application of the methods under the above.

(1) Documents shall be kept in the general order of all documents and records kept in the IP. Documents received electronically, together with the contract accepted by the client and given a unique number, together with declarations and other additionally requested documents, shall be stored in an electronic file and/or on paper, and electronic messages sent and received shall be stored electronically.

Art. 27. In the course of an already established business relationship, when the identification has been carried out at the entry into such relationship, the documents submitted at the time of the identification shall be periodically re-requested and checked for any change in the identification data in accordance with the Procedure for Updating Customer Data, annexed to these Internal Rules.

Art. 28. The actions undertaken pursuant to Articles 24 to 27 shall be documented and the documents relating to the verification of the identification shall contain information on the date and time of the verification, as well as the name and position of the person who carried it out.

Identifying the beneficial owner of the client and verifying identification

Art. 29. The identification of the beneficial owner of the client shall be carried out before the establishment of a business relationship, the execution of a casual transaction or the conclusion of a casual transaction.

Art. 30. The Company shall identify any natural person who is the beneficial owner of a client - a legal person or other legal entity, by collecting data on:

1) names;
2) date and place of birth;
3) an official personal identification number or other unique element of identification contained in an official identity document which has not expired and which bears a photograph of the client;
4) any nationality the person holds;
5) country of residence and address (a PO Box number is not sufficient).

Art. 31. Data on the beneficial owner shall be collected by:

1) Reference to the accounts of legal entities and other legal entities established on the territory of the Republic of Bulgaria in the Commercial Register, in the Register of Non-Profit Legal Entities and in the BULSTAT Register;
2) Reference to the relevant public register of the legal entity's account - if there is an official public commercial or company register in the Member State where the legal entity is registered;
3) Submission of an original or notarized copy of an official extract from the relevant register of current status, a certified copy of the memorandum of association, the articles of incorporation or any other document necessary to establish the data referred to in Article 30;
4) a certificate, contract or other valid document under the law of the jurisdiction in which the client is incorporated, from a central registry or registrar, showing who the beneficial owners of the client are, being a body corporate or other

legal entity with nominee directors, nominee secretaries or nominee owners of the capital ;

5) IP “INTERCAPITAL MARKETS” AD shall require a declaration of beneficial owner in accordance with Annex 4 of the AML/CFT Regulations in cases where the information collected through the means under Article 31 (1) - (4) is insufficient to identify the natural person who is the beneficial owner of a client - a legal person or other legal entity, as well as where the application of the means under (1) - (4) has resulted in contradictory information.

Art.32. For clients legal entities whose shares are traded on a regulated market, which are subject to disclosure requirements in accordance with the law of the European Union or equivalent international standards ensuring an adequate degree of transparency with respect to ownership, the Company shall collect the information on the shareholding subject to disclosure under Chapter Eleven, Section I of the Public Offering of Securities Act, or similar information concerning companies on a regulated market outside the Republic of Bulgaria.

Art. 33. The information collected shall be stored in the client file in the order specified in Section VII.

Verification of the identification of the beneficial owner

Art. 34. Verification of the identification of the beneficial owner of the client shall be carried out taking into account the level of risk arising from the establishment of the client relationship and/or from the conduct of transactions or operations with that type of client. For this purpose, the actions pursuant to Article 24 et seq. of these Internal Rules shall be taken.

Rules when establishing a business relationship or carrying out a casual operation or transaction without the client being present

Art. 35. In the event of establishing a business relationship or carrying out a casual operation or transaction without the presence of the client, a copy of an identity document shall be required for identification.

Art. 36. The verification of the identification made shall be carried out by applying two or more of the methods referred to in Article 24 of the Internal Rules.

Art. 37. The Company shall use an internal control system in accordance with Article 41(2) of the the AML/CFT Regulations, which shall limit the risks arising from the remote nature of identification and its verification.

Art. 38. The internal system shall be used to limit the possibility of:

1) provision of false identification data by the identifiable natural person
2) the use of foreign identification and identity documents.

Art. 39. The internal control system of the Company shall provide:

1) Identification of changes or damage to security features and their placement on identity documents by the Company employee;
2) clarify the reasons why a client from another country or jurisdiction uses the Company's services;

3) applying restrictions on the documents accepted by applying at least two of the following requirements:

- acceptance of official identity documents containing security features only;
- acceptance of official identity documents containing biometric data only;
- acceptance only of official identity documents issued by a competent authority of the Republic of Bulgaria or another Member State;
- accepting only official identity documents containing a photograph of the person to be identified and a unique document number;
- a requirement to use a qualified electronic signature;
- a requirement to send an electronic statement within the meaning of the Electronic Document and Electronic Trust Services Act (EDETSA).

4) Traditional means of communication may also be used to verify identification, such as sending a letter to the address on the identity document, conducting a telephone conversation, exchanging electronic messages by e-mail specified by the client (individual), and other reasonably applicable means.

5) In case the verification of the identification carried out under point 4 proves insufficient for the purposes of limiting the risks of money laundering or terrorist financing, the IP may organise a video conference with the person to be identified. The video conference shall meet the following conditions:

- the conversation with the person to be identified should be conducted by a trained officer;
- the conversation to take place in a separate room;
- require the explicit prior consent of the identifiable person for identification and verification of identification;
- the light to be appropriate;
- the conversation to take place in real time;
- take a picture of the client's face as well as the face and back of the identity document.

6) At the discretion of the person exercising internal control over the fulfilment of the obligations of the AML Act and the AML/CFT Regulations, the IP may use other technical means to verify the authenticity and reliability of the identity documents provided by the client, respectively its representative, when concluding contracts in connection with the activities of the IP.

Reference to previous identification

Art. 40. (1) IP "Intercapital Markets" AD may rely on a previous identification of the client made by a credit institution for the purposes of the client due diligence in the presence of the following cumulative conditions:

1. the head office of the credit institution that has made the identification is in the Republic of Bulgaria, in another Member State or in a third country whose legislation contains requirements that comply with the requirements of the AML/CFT Act, taking into account the level of risk of these countries and the implementation of **measures** to counter money laundering and terrorist financing in accordance with this level, the availability of the

full range of such measures in accordance with the requirements of the Financial Action Task Force on Money Laundering (FATF) and their effective implementation;

2. the information required by Articles 15 and 16 of the Internal Information Rules shall be available to the investment firm and copies of the documents and information collected may be obtained immediately upon request.

3. upon request, the credit institution that has made a previous identification shall be able to provide, within three days, to the person claiming such identification, certified copies of the documents referred to in point 2.

(2) IP "Intercapital Markets" AD may not rely on a previous identification of the client made by a credit institution from a high-risk third country under Art. 46, para. 3 of the AML Act.

Reference to previous identification within the group:

Art. 41. An IP may rely on prior identification of the client, or its beneficial owner, in applying policies and procedures within the group, subject to the following cumulative conditions:

1. The IP relies on information provided by a third party that is part of the same group;
2. The Group implements client due diligence measures, record retention policies and anti-money laundering and anti-terrorist financing programmes in accordance with the AML/CFT Act;
3. The effective implementation of the AML/CFT requirements shall be supervised at group level by a competent authority.

Acting on behalf of another person

Art. 42. (1) In cases where a contract is concluded through a legal representative or proxy, the IP shall establish their representative authority and shall carry out identification of the representative or proxy as well as of the client in accordance with Art. 15 above and subject to the requirements of Art. 59 of Regulation No. 38.

(2) Where there is any doubt that the person entering into the contract with the IP is not acting in his own name and on his own behalf, the IP shall make a notification and take one or more of the following actions to gather information to identify and verify the identity of the person in whose favour the contract is actually being entered into:

1. carries out extensive ongoing monitoring of the operations and transactions carried out within it;
2. review the documents, data and information collected in the course of the due diligence on the client and its beneficial owner;
3. requires additional documents;
4. makes inquiries in publicly accessible local and foreign official commercial, company and other registers;
5. consult publicly available sources of information;
6. exchange information within the group;

7. requires confirmation of identification from another person obliged under the AML Act or from a person obliged to implement anti-money laundering measures in another Member State or in a Trusted Third Country;

Clarification of the origin of funds

Art. 43. (1) The IP shall clarify the origin of the client's funds by applying at least two of the following methods:

1. collecting information from the client about its core business, including the actual and expected volume of business and the transactions or dealings expected to be conducted within that relationship, by completing a customer questionnaire;
2. collecting other information from official independent sources - data from publicly available registers and databases, etc;
3. use of information collected in connection with the implementation of the requirements of the AML Act or other laws and regulations, including the Foreign Exchange Act (to the extent applicable to the transactions and operations carried out by the IP), that shows the clear origin of the funds;
4. use of information exchanged within the group to show the clear origin of funds;
5. tracking cash flows within the established business relationship with the client, where the origin of funds is clear.

(2) Where it is impossible to clarify the origin of the funds after exhausting the means under par. 1, and in cases where the application of at least two of the means under par. 1 has resulted in contradictory information, the clarification of the origin of the funds shall be carried out by means of a written declaration by the client or his legal representative or proxy. Clarification of the origin of the funds may be made by means of a written declaration in the form provided by the client or by his/her legal representative or proxy where the application of two of the means referred to in paragraph 1 has been inconsistent.

Ongoing monitoring

Art. 44. The IP shall carry out ongoing monitoring of the established business relationship with the client and the transactions and operations carried out within the same, in order to timely identify the presence of any of the risk factors specified in these Internal Rules and take the necessary measures for the prevention and management of the risks of money laundering and terrorist financing in these cases.

Measures for enhanced client due diligence, respectively the actual owner of the customer.

- General measures for extended due diligence

Art. 45. (1) The IP shall apply measures for extended due diligence in the following cases:

1) when entering into a business relationship with a prominent political figure and in the course of such a relationship, as well as when conducting a casual transaction or deal with a prominent political figure;
2) when entering into a business relationship and during the course of such a relationship, as well as when carrying out an incidental transaction or dealing with customers established in high-risk third countries;
3) in complex or unusually large transactions or operations, as well as operations and transactions without an apparent economic or legitimate purpose;
4) unusual scheme, justification of transactions and operations
5) receiving/ordering transfers to high-risk countries
6) unusual payments from third parties
7) in all other cases where the risk assessment or the National Risk Assessment identifies a higher risk of money laundering, terrorist financing and/or the presence of funds of criminal origin;

Art. 46. The Company, as an obliged person under the MAML Act, shall apply the enhanced due diligence measures in respect of prominent political figures (in the Republic of Bulgaria, in another Member State or in a third country) who are potential, existing clients and beneficial owners, as well as in respect of persons related to them.

Art. 47. The Company shall carry out a risk assessment of the business relationship with the client in order to assess the need for the continued application of one or more of the enhanced due diligence measures where a person has ceased to hold office as a prominent political figure for a period of not less than 1 year.

Art. 48. The IP shall apply the following general measures for enhanced due diligence:

1. requiring and/or collecting a larger volume of data, documents and information;
2. requesting data, documents and information from various sources in order to collate, collect and/or verify data, documents and information already collected;
3. taking into account the frequency with which the actions referred to in points 1 and 2 are carried out in relation to the identified level of risk of money laundering and terrorist financing;
4. Requiring authorization from the Head of the IP Specialized Office to establish or continue a business relationship, and to conduct certain transactions or operations within the business relationship or to authorize the use of particular products or services, business practices, delivery mechanisms, and the use of new technologies;
5. clarification of the sources of the client's assets;
6. requesting references from the client's counterparties or other persons obliged under the AML Act;
7. commissioning of investigations or other actions necessary for this purpose to persons of good repute and with proven expertise and practical experience in the prevention and suppression of money laundering and terrorist financing;

Identifying Prominent Political Personalities

Art. 49. The Company shall develop and implement an internal system to identify prominent political figures who are potential clients, existing client or actual client owner.
Art. 50. The Company shall determine whether a prospective client, existing client or beneficial owner is a Prominent Political Figure using one of the following sources of information:

1) completion of a declaration of a Prominent Political Personality under Article 41, paragraph 2, item 2 of the AML Act by the client;
2) information obtained through the enhanced due diligence measures;
3) verification of the information declared by consulting public registers and information databases containing information on the different categories of prominent political figures.

Art. 51. The IP shall use at least two of the following means to establish whether the client or its owner is an PPP when:

1) the client or the beneficial owner of the client is from a country where there is information of high levels of corruption or from a country subject to sanctions, embargoes or similar measures by the European Parliament and the Council or the United Nations Security Council, or in cases of specific instructions from the European Union or the United Nations;
2) the client, a legal person or other legal entity, has an ownership structure that includes nominee owners and managers or otherwise makes it difficult to identify the beneficial owners and/or assumes anonymity;
3) where there is no real activity in the country and/or where the account is primarily used to transfer funds between other persons;
4) in the event of a partial identity match with persons for whom negative information is available in databases or information from open sources;
5) when a higher risk is identified according to the Risk Assessment of IP "Intercapital Markets" AD.

Application of enhanced due diligence measures to prominent political figures

Art. 52. (1) The following measures shall apply to the conclusion of a contract with clients who are prominent political figures or persons related to prominent political figures, including clients whose beneficial owner is a prominent political figure or a person related to a prominent political figure:

1) Approval of the Head of the Specialist IP Office is required. The approval shall state the full identification details of the person referred to in Article 36 of the AML Act and the position held in the institution concerned. The document must be signed by a senior official. The IP shall keep all documents, data and information collected and produced in accordance with the rules of Section VII of the Internal Rules for the Control and Prevention of Money Laundering and Terrorist Financing.

2) In cases where, after entering into a contract with a client, it is determined that the client or its beneficial owner is a Prominent Political Figure or a person associated with a Prominent Political Figure, the continuation of the business relationship with that client may only take place after approval has been obtained.

(2) The IP shall establish, in accordance with these Rules, the ***origin of the funds*** used in the business relationship and the operations and transactions carried out on the basis of a contract concluded with a client who is a prominent political figure or a person related to a prominent political figure or whose beneficial owner is a prominent political figure or a person related to a prominent political figure. The IP shall take appropriate action to clarify the ***source of the assets*** of a client or beneficial owner of a client, a PPP or a person associated with a PPP by periodically reviewing and comparing the information about the declared assets of the client or beneficial owner of the client with the information established as a result of the application of the due diligence measures.

(3) The IP shall conduct ***ongoing and extended monitoring of its business relationship*** with a client that is a Prominent Political Figure or a Prominent Political Figure's affiliate, or whose beneficial owner is a Prominent Political Figure or a Prominent Political Figure's affiliate, in order to assess whether there has been a material change in the type, value, volume, frequency, amount and manner of transactions and dealings that could affect the level of identified risk.

Art. 53. The actions of the IP under Article 52 shall be documented and updated in accordance with the Client File Update Procedure, annexed to these Internal Rules.

Art. 54. The measures referred to in this Article shall not apply in the event that the client, respectively his beneficial owner, has ceased to hold the office which served as the basis for his designation as a Prominent Political Personality for a period of not less than one year. After the expiry of the period referred to in the preceding sentence, the IP shall carry out a risk assessment of the business relationship with the client with a view to assessing the need to continue to apply one or more of the enhanced due diligence measures. The assessment shall be documented and stored in accordance with Section VII and updated in accordance with the risk profile of the client.

Measures for complex or unusually large transactions or operations, as well as transactions and operations with no apparent economic or legitimate purpose

Art. 55. Where complex or unusually large transactions or operations, or transactions and operations without an apparent economic and legitimate purpose are carried out by a client, the IP shall undertake the following specific enhanced due diligence measures to assess whether they constitute suspicious transactions or operations:

1. Ongoing and extended monitoring of all complex or unusually large transactions or operations, as well as all transactions and operations that have no apparent economic or legitimate purpose that can be ascertained from information available to the IP, or are inconsistent with available client information.
2. Assessment of the transactions and operations based on the information gathered on their nature, their consistency with the client's usual business and its object, the value of the transactions and operations, their frequency, the financial situation of the client, the means of payment used, as well as on other indicators specific to the type of activity concerned.
3. Gather information on the essential elements and value of the transaction or transaction, relevant documents and other identifying data. The IP shall document its judgement as to the existence of the conditions for reporting under Article 72 of the AML Act as a result of the information collected.

Determination of measures for extended due diligence

Art. 56. (1) The IP shall determine the type of specific enhanced due diligence measures (general and specific), as well as their extent and scope, in accordance with the identified risk of money laundering and terrorist financing in each specific case.

(2) The IP shall duly document the actions carried out to establish the existence of the circumstances, conditioning the application of the measures for extended due diligence and shall store the collected data, documents and information in accordance with Section VII.

Supplementary rules for the application of the measures under the AML Act in the activities of investment brokers

Art. 57. In the course of the IP Activity:

1. According to the current regulations applicable to the activity of the IP, the same cannot act on behalf of a client without having identified the client in advance. Therefore, it is not allowed to anonymously carry out operations and transactions on the part of the client or to allow a third party to have a decisive influence on the use of services and the conclusion of transactions.
2. According to its internal rules, the IP does not accept payments (client deposits and withdrawals) in cash.
3. According to the current regulations applicable to the activity of the IP, the same may not act on behalf of a client without having previously concluded with the client a contract for the provision of investment and/or additional services. Therefore, the execution of random transactions and operations by the client is not permissible.

VI. SPECIALIZED SERVICE. SYSTEM FOR INTERNAL CONTROL

Art. 58. (1) The IP shall establish a specialized office under Art. 106 of the AML Act, designated by order of the governing body, which shall prepare, propose for approval and implement training programs for employees on the implementation of the AMl Act, its implementing acts and these rules and shall organize, manage and control the activities on:

1. collecting, processing, storing and disclosing information about specific operations or transactions;
2. gathering evidence on the ownership of the property to be transferred;
3. requesting information on the origin of the cash or valuables that are the subject of the operations or transactions and on the source of the assets;
4. collecting information on clients and maintaining accurate and detailed records of their transactions in cash or valuables, including the information and documents referred to in Article 6 of the Currency Act;
5. providing the collected information to the Financial Intelligence Directorate of the State Agency for National Security.

(2) The system for internal control over the fulfilment of obligations under the AML Act is based on (and documented through) the completion of checklists.
(3) When a new employee is appointed, a checklist shall be completed in accordance with Annex I;
(4) For the purpose of carrying out annual internal control over the implementation of the obligations under the AML Act, a check-list in accordance with Annex II shall be completed within the time limits set out in Articles 28 and 54.
(5) The Head of the Specialised Service shall be responsible for the internal control of the implementation of the obligations under the AML Act, the AML/CFT Regulations and these Rules. The Head shall be appointed by order of the management body of the IP.

(6) The IP may establish a specialized service under the conditions and in accordance with the procedure of Article 106 of the AML Act by a written act. In this case, the IP shall, within 7 days of the designation or replacement of the officer responsible for the internal control of the performance of the obligations under the AML Act, notify the Financial Intelligence Directorate of the State National Security Agency of the name of the officer, as well as provide contact details for the officer.

VII. INFORMATION RETENTION AND DISCLOSURE. OVERVIEW AND DATABASE UPDATE

Storage of documentation

Art. 59. The IP shall keep all documents, data and information collected and prepared under these Rules for a period of 5 years from:

1. With respect to documents prepared and received in connection with established business relationships with clients, the date of termination of the relationship
2. In the case of disclosure of information pursuant to Article 37 of this Section, from the beginning of the calendar year following the year of disclosure of the information.
3. For documents prepared in connection with the Risk Assessment under Section IV and V, from the beginning of the calendar year following the year of their preparation.

(2) Upon written instruction of the Director of the Financial Intelligence Directorate of the State National Security Agency, the period for the retention of documents may be extended by not more than two additional years.

(3)The IP shall retain the documents prepared and received in connection with these Rules throughout the duration of its activities and for a period of one year from the cessation thereof.

(4)All documents, data and information collected and prepared by the IP in accordance with these Rules shall be stored in a manner that:

1. Allows for their timely recovery in the event that they are to be made available for use as evidence in judicial and pre-trial proceedings.

2. Ensures that they are available to the Financial Intelligence Directorate of the State National Security Agency, the relevant supervisory authorities and the auditors. The documents, information and data shall be made available to the Financial Intelligence Directorate of the State National Security Agency upon request in original, certified copy, extract or reference within the time and in the format specified by the Director of the Directorate.

Disclosure of information

Disclosure of information on suspicion of money laundering

Art. 60. (1) In case of suspicion and/or knowledge of money laundering and/or of the presence of funds of criminal origin, the IP shall immediately notify the Financial Intelligence Directorate of the State National Security Agency prior to the execution of the relevant operation or transaction, delaying its execution within the permissible period under the regulations governing the relevant type of activity. In the notification under par. 1, the IP shall indicate the maximum period within which the operation or transaction may be delayed.

(2) Upon becoming aware of money laundering or the presence of funds of criminal origin, the IP shall also notify the competent authorities in accordance with the Criminal Procedure Code, the Law on the Ministry of Interior and the Law on the State National Security Agency.

(3) Where the delay of the operation or transaction referred to in par. 1 is objectively impossible or is likely to frustrate actions to pursue the beneficiaries of a suspicious transaction or operation, the IP shall notify the Financial Intelligence Directorate of the State National Security Agency immediately after the transaction or transaction has been carried out, stating the reasons why the delay was impossible.

(4) The notification of the Financial Intelligence Directorate of the State National Security Agency shall be made by the Head of the Specialized Service of the IP, in a form approved by the Director of the Financial Intelligence Directorate of the State National Security Agency. Notification may also be made by other IP staff.

Register

Art. 61. (1) The IP shall maintain a special register in which it shall keep:

1. any report by an employee of a suspicion of money laundering or of the presence of funds of criminal origin, irrespective of the manner in which the report is made, together with a conclusion as to the need to report the suspicion;

2. a conclusion as to the purpose and nature of complex or unusually large operations and transactions, and a conclusion as to the existence of suspicion of money laundering or the presence of funds of criminal origin in those cases.

(2) The register shall be kept on paper, which shall be stamped, numbered and authenticated by the signature of the Head of the Specialised Service and the seal of the Company.

(3) (amended 19.11.2021) The person designated to exercise internal control over the performance of the obligations under the AML Act and its implementing regulations shall be responsible for the proper maintenance and preservation of the register and shall strictly monitor compliance with the legal requirements for the maintenance of the register. When a report is entered in the register, the person to whom the report is made shall open a file in which all documents relevant to the actions carried out by the IP's employees in connection with the report of suspected money laundering and the relevant complex or unusually large transactions and dealings shall be collected and filed in the order of their receipt.

Updating the databases

Art. 62. (1) The IP shall keep up-to-date the information on its clients and on the operations and transactions carried out by them by periodically reviewing and updating, if necessary, the maintained databases and client files in accordance with the Procedure for Updating Client Files (Annex to these Internal Rules). The review referred to in the preceding sentence shall be carried out as follows:

0000002330	0000002330
Low	at 2 years
Medium	at 1 year
High	at 6 months

(2) Regardless of the periodic update, the IP shall verify and additional identification and verification actions shall be performed whenever:

1. a transaction has been entered into at a value materially different from the client's usual value;
2. there is a significant change in the way the open account is used or in the way certain transactions or dealings are carried out;
3. the IP becomes aware that the information it has on an existing client is insufficient for the purposes of applying the due diligence measures;
4. the IP becomes aware that there has been a change in the circumstances established by the application of the due diligence measures in respect of the client.

Updating the risk assessment

Art. 63. (1) The IP shall review and, if necessary, update the IP-specific money laundering and terrorist financing risk assessment every two years. The review and update shall take into account the Supranational and National Risk Assessment as well as the recommendations of the European Commission.

(2) Notwithstanding the review and update periods referred to above, the IP shall take immediate action to update the assessment referred to in paragraph (2) where, in applying the due diligence measures, it identifies a discrepancy between the information about the client, the transactions and the operations and the nature and purpose of the established business relationship and/or the risk identified in relation to the business relationship with the client.

VIII. ALLOCATION OF RESPONSIBILITIES

Art. 64. The overall responsibility for the performance of the obligations of the IP, in accordance with the AML Act, the AML/CFT Regulations and these Rules shall be borne by the Board of Directors of the IP.

1. Board of Directors of the IP:

- Accepts these Rules
- Appoint and dismiss the Head of the Specialised Service and the person discharging the duties under the AML Act for the branch of the Investment broker
- Provide overall monitoring and guidance in relation to the IP's compliance with its obligations under the AML Act, AML/CFT Regulations and these Rules.

(2) The Specialised Service shall have the duties and responsibilities set out in Section VIII of the Rules.

(3) The Head of the Specialised Service shall continuously monitor the fulfilment of the obligations of the IP under these Rules. In the event of irregularities being detected, the Head of the Specialised Service shall prepare a report to the Board of Directors of the IP, with a proposal to take specific measures to mitigate the consequences of the deficiencies and to prevent future ones and, if necessary, to amend these Rules.

(4) The persons referred to in Article 65 of Regulation No 38 who conclude contracts with clients on behalf of the IP and accept orders to enter into transactions in financial instruments shall be responsible for applying due diligence measures (standard due diligence measures, general due diligence measures or specific due diligence measures) according to the identified level of risk in relation to the business relationship with the specific client.

(5) The IP's accounting staff is required to monitor for the presence of any of the criteria for suspicious transactions and operations in servicing payments made to and from the IP in relation to the investment services and activities performed.

(6) All employees of the IP are obliged to provide the necessary assistance to the specialised service and to monitor, in accordance with their level of competence and the specific functions assigned within the IP, the existence of any of the criteria for suspicious transactions and operations in relation to the investment services and activities carried out by the IP.

IX. EMPLOYEE TRAINING

Art. 65 (1) The IP shall ensure that induction, ongoing (continuing) and specialised (ad hoc) training is provided to the specialised service and other IP staff, under the conditions and within the timeframes set out in the IP Staff Training Plan in relation to the implementation of anti-money laundering measures. The plan shall be updated annually.

1. The Head of the Specialised Service and all employees are obliged to continuously improve their competence in the field of anti-money laundering prevention by keeping up to date with the latest legal requirements, guidelines issued by European and local supervisory authorities and established best practices in this area. The Head of the Specialised Service or his/her designees shall attend, whenever possible, specialised seminars and trainings organised by the Financial Intelligence Directorate of the State National Security Agency.

2. All employees shall complete a declaration that they are aware of these Internal Rules and undertake to comply with them. These declarations shall form an integral part of the employment records.

X. INTERNAL SIGNALS

Art. 66. Any employee of the IP may submit a report, including anonymously, in case of suspicion of money laundering, to the person who carries out the internal control of the implementation of the obligations under the AML Act and the Regulations for its implementation of the IP at the address of the management of the IP. The IP shall guarantee the anonymity of the employees who have reported under the previous sentence.

(2) The Head of the Specialised AML Service shall immediately record the alert received in the register referred to in Article 61 above.

(3) The Head of the Specialised AML Service shall immediately examine the report received, make the necessary assessment of the case and, if necessary, make a notification under Article 61 above. The verification by the person exercising internal control over the implementation of the obligations under the AML Act and its implementing rules and the assessment made shall be documented and kept in accordance with Section VII of these Rules.

XI. FINAL PROVISIONS

§1. These Internal Rules have been adopted by a resolution of the Board of Directors of IP dated 22.12.2021 and repeal the previous ones adopted on 31.03.2021.

§2 The Rules are subject to annual review by the Head of the Specialised Service. In the event of any deficiencies in the Rules identified during the review, necessary changes shall be made.

§ 3 These Internal Rules shall apply accordingly to the branches of the Investment Broker in the country and abroad.

ANNEXES:

ANNEX I -CHECKLIST FOR NEW EMPLOYEES
ANNEX II - ANNUAL INTERNAL CONTROL CHECKLIST
ANNEX III - REPORTING ON SUPRANATIONAL AND NATIONAL RISK ASSESSMENT

Annex I

CHECKLIST FOR NEW EMPLOYEES

1. EMPLOYEE (NAMES):	2. PERSONAL IDENTIFICATION NUMBER: .....
3. THE FOLLOWING ACTIONS HAVE BEEN CARRIED OUT IN THE APPOINTMENT OF THE EMPLOYEE: [ ] Induction training of the employee on the application of the AML/CFT Act, the AML/CFT Regulations, the Internal Rules under the AML Act and the related implementing internal acts. [ ] A Training Report has been signed for the training provided.	
4. THIS CHECKLIST IS COMPLETED BY: Names: ..... Date: ..... Signature:	

Annex II

ANNUAL INTERNAL CONTROL CHECKLIST

IN THE ANNUAL INTERNAL CONTROL ON THE IMPLEMENTATION OF THE OBLIGATIONS UNDER AML FOR 2021, THE FOLLOWING ACTIONS WERE CARRIED OUT:
1. ON CLIENT RECORDS: [ ] Number of client records check - ..... [ ] Number of updated information in client records - .....

2. IMPLEMENTATION OF THE ANNUAL STAFF TRAINING PLAN:

[ ] Annual staff training plan adopted

[ ] Number of induction trainings for employees - .....

[ ] Number of continuing training of employees - .....

[ ] Total number of employees trained - .....

3. IN RELATION TO RISK ASSESSMENT:

A. Review of the obligor's own risk assessment [ ]No [ ] Yes

B. Update of the obligor's own risk assessment [ ] No [ ] Yes

C. A change in the level of risk identified in the risk profiles of clients:
from 'high' to 'medium' or to 'low' - [ ] No [ ] Yes: .....

from 'medium' to 'low' or to 'high' - [ ] No [ ] Yes: .....

from 'low' to 'medium' or to 'high' - [ ] No [ ] Yes: .....

D. A review of the transactions and dealings carried out in the course of a business relationship with a client who is identified as, or the beneficial owner of, a prominent political figure or a person associated with such a figure (a person referred to in Article 36 of the AML) - [ ] No [ ] Yes: ..... number of business relationships

E. Relationship review and risk reporting performed on clients and beneficial owners of clients who have been identified as persons under Article 36 of the AML, but have ceased to hold the relevant position - [ ] No [ ] Yes: ..... number of business relationships

4. THE ACTIONS ON THIS CHECKLIST HAVE BEEN CARRIED OUT BY NIKOLAY MAISTER

Date: _____ Signature: _____

Annex III

CONSIDERATION OF SUPRANATIONAL AND NATIONAL RISK ASSESSMENT

In preparing the Risk Assessment, in accordance with its obligations under Article 99 of the AML Act, the IP should consider and take into account the results of the Supranational Risk Assessment (SNRA) and the National Risk Assessment (NRA).

1. Supranational Risk Assessment

The ML/TF SNRA is carried out by the European Commission on the basis of Article 6 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (the Fourth Directive). The assessment concerns the entire internal market of the European Union and is carried out at least every two years.

The SNRA at the time of adoption of this Risk Assessment (RA) consists of:

- Report from the European Commission to the European Parliament and the Council on the assessment of money laundering and terrorist financing risks affecting the internal market and related to cross-border activities COM(2017) 340 final of 26.06.2017 (the 2017 Report);[1] .
- Report from the European Commission to the European Parliament and the Council on the assessment of money laundering and terrorist financing risks affecting the internal market and related to cross-border activities COM(2019) 370 final of 24.07.2019 (the 2019 Report)[2] ;

1.1. 2017 Report.

In Section 2 Results of the 2017 Report, the European Commission (EC) states that "the financial sector has been covered by the EU's AML/CFT framework since 1991 and the seems to have a good awarness of its risks. While terrorists and criminals are still trying to use the financial sector for their activities, the assessment show that the level of ML/TF risks

[1] https://ec.europa.eu/transparency/regdoc/rep/1/2017/BG/COM-2017-340-F1-BG-MAIN-PART-1.PDF .

[2] https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf .

to the financial sector is moderately significant due to the mitigating measures already in place.
However, the risk of money laundering remains significant for certain segments in the financial sector, such as private banking and institutional investment (especially through brokers). This is due to the overall higher exposure to product and customer risks, pressures of competition in the sector and a limited understanding among supervisors of their operational AML/CFT risks.

In its recommendations under item 4, the EC states that it should "analyse operational AML/CFT risks linked to the business/business model in the corporate banking, private banking and institutional investment sectors on the one hand, and in money value transfer services and e-money on the other."

In view of the above, the Company acknowledges the European Commission's view that its business may be exposed to risks from ML/TF that have not yet been fully considered and investigated.

1.2. 2019 Report

The 2019 Report takes into account the amendments to the Fourth Directive regime introduced by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (the Fifth Directive).

The 2019 Report refers to the conclusions drawn by the European Supervisory Authorities' (ESAs) General Opinion on money laundering and terrorist financing risks affecting the financial sector of the European Union[3]. In item 5.8 of the Opinion, concerning investment brokers, the ESAs note that

- The most significant risks of ML/TF come from clients who are not citizens/residents of the country where the IP is established and transactions without the presence of the client, especially in relation to clients who are established in countries or geographic areas with preferential tax regimes;
- Specific new risks relate to innovation and the use of new technologies in the sector, such as those used in connection with high-frequency algorithmic trading, peer-to-peer lending activities, initial coin offerings and virtual currencies.

1.3. Compliance with the results of the SNRA

The Company fully acknowledges and adopts the findings of the SNRA and will take them into account when conducting transactions or establishing business relationships with clients.

2. National risk assessment

[3] https://esas-joint-committee.europa.eu/Publications/Opinions/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf .

2.1. Summary of the NRA

The summary of the national risk assessment was published on the website of the State National Security Agency (SNSA) on 9 January 2020.

In the summary of the NRA, SNSA states that:

"In the financial instruments in investment sector, non-bank investment brokers operating online trading platforms appear to be the highest risk for money laundering internationally due to their relatively high turnover, very wide geographical diversification and the shortcomings of non-present identification of clients, as well as the formal application of some of the requirements of the AML/CFT legislation. Associated risks include scenarios for the layering of funds obtained from predicate offences committed abroad."

2.2. Summary list of major risk events

The SNSA has published a Summary List of the main risk events identified through the NRA and includes the following risk events that may affect the activities of the IP:

i. Scenario 22 indicates that OTC securities transactions through investment brokers in many cases involve "layering" or "integration" phases of funds with different criminal origins. Securities transactions through investment brokers are in certain cases linked to fraudulent privatisation or the use of funds of illicit origin.

ii. Scenario 23 indicates that there are indications of a significant development in the use of financial instruments based on new technologies and emerging trading conditions, and insufficient regulatory response (not only at the local level, but also at the European and at international level). In many cases, non-residents are involved and the schemes only partially affect the Bulgarian financial system in some aspects (usually placement and layering). At the same time, the immature securities market and investors' lack of tradition and skills contribute to various types of financial instrument fraud linked to the operations of unlicensed companies.

iii. Scenario 25 indicates that trading financial instruments through investment brokers carries some risk arising from the relatively high transaction amounts and some significant vulnerabilities associated with both the investment brokers and some contextual factors. Nonetheless, the low level of market development, as well as the more difficult market access and operational opportunities, would limit the potential impact of the threat. No actual cases have been observed.

The following risk events from the Summary List may also affect the activities of the IP and should be taken into account in the risk assessment:

i. Money laundering from a wide range of predicate offences committed abroad or within the country related to organised crime (mainly drugs, human trafficking and tax crimes such as tax evasion) through the use of the formal financial system and the extensive use of cash;

ii. Money laundering of proceeds of corruption (incl. property acquired through misappropriation of funds / fraudulent procurement of EU funds) through

sophisticated money laundering schemes within or outside the country using "professional launderers" and the subsequent integration of the funds into financial instruments abroad and into legal entities and real estate in the country;

iii. Money laundering from tax crimes (tax evasion and VAT fraud) through the use of 'frontmen', domestic and foreign legal entities in complex layering schemes and with the help of "professional launderers";

iv. Laundering of proceeds of tax crime (tax evasion and VAT fraud) in the food and fuel trade through the use of shell companies and nominee owners, facilitated by the environment of corruption and the informal economy;

v. The possible involvement of professionals and obliged entities under the AML Act facilitated by vulnerabilities related to market access rules (e.g. registration/licensing) and the selection of their employees, as a key risk that facilitates the functioning of organised crime and contributes to the level of most of the risks listed above.

2.3. Compliance with the results of the NRA

The Company acknowledges the findings of the NRA that the services offered within its business and the mechanisms for their delivery carry with them an inherent risk of ML/TF. The Company will take these into account when conducting transactions or establishing business relationships.

The Company fully accepts the conclusions and recommendations made in the NRA and will take them into account in preparing the risk assessment under Article 98 of the AML Act below.