Translation from Bulgarian into English

INTERNAL RULES
ON MONEY LAUNDERING AND TERRORIST FINANCING CONTROL AND PREVENTION OF IP INTERCAPITAL MARKETS AD

I. GENERAL

Art. 1. (1) These Internal Rules (hereinafter reffered to as the "Rules") are developed on the basis of Art. 101, para. 1 of the Law on Measures against Money Laundering (LMML) and in connection with the National Risk Assesment adopted on 09 January 2020 under Art. 95 of the LMML.

(2) **IP INTERCAPITAL MARKETS AD**, registered in the Commercial Register at the Registry Agency with UIC: 131057477 (hereinafter reffered to as **"IP"**), applies the measures provided for in the LMML as an intermediary broker holding license No. RG-03-0204/24.02.2006 issued by the Financial Supervision Commission (FSC) – an obliged person under Art. 4, item 8 of the LMML.

Art. 2. The purpose of these Rules is to ensure the effective performance of the obligations of the IP, in accordance with the LMML and the Rules on the implementation of the LMML (RILMML), 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 IB level.

II. DEFINITIONS

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

"Promenient 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 ot 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 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 apply or do not fully apply the international standards in anti-money laundering defined by the European Commission by Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Paliament and of the Council by identifying high-risk third countries with strategic weaknesses and identified in a list on the websites of the State Agency for National Security, the Bulgarian National Bank, the Financial Supervision Commission, the National Revenue Agency and the Ministry of Finance.

"High-risk jurisdictions" are those jurisdictions listed 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 entitied in which the parent undertaking or its subsidiaries have an interest, and undertakings related to each other within the meaning of Art. 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 establishing contact it is assumed 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, item 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. dealing 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 transactins in financial instruments;
6. Underwriting services for financial instruments;
7. Investments 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 acillary services.

"Money laundering" is:

1. Conversion or transfer of property, with knowledge that such property has been acquired from a criminal activity or from an act of participation in a criminal activity, 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 was derived from a criminal activity or from an act of participation in a criminal activity;

3. Acquisition, possession, holding or use of property, knowing at the time of receipt, that such property was derived from criminal activity or from an act of participation in a criminal activity;

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 promenient political figure" means persons who have the following relationships with a promenient 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 fecto conjugal relationship;

3. First-degree ascendants and their spouses or persons with whom the first-degree ascendants live in de fecto conjugal relationship;

4. Second-degree collateral relatives and their spouses or persons with whom the second-degree collateral relatives live in de fecto conjugal relationship;

5. Any individual who is known to be the actual owner, jointly with a promenient political figure, of a corporation or other legal entity or is otherwise in a close business, professional or other business relationship with a promenient political figure;

6. Any natural person who is the sole owner or actual owner of a corporation or other legal entity known to have been formed for the benefit of a promenient political figure.

"Reliable 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.

"Reliable third country" – a third country (i.e. a Non-Member State) whose legislation contains requirements consistent with the requirements of the LMML, taking into account the level of risk of those countries and the implementation of anti-money laundering and counter-terrorist financing (AML/CFT) measures consistent with the FATF requirements and their effective implementation.

"Ordinance No. 38" – Ordinance No. 38 of 21 May 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 Art. 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 borders, 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, para. 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;
- Certificate for travelling abroad of a refugee;
- 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 affixed 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) 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 operations" 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 LMML, or

b) a series of transfers through different entities reffered to in Art. 4 of the LMML which is related to the same obligation, or

c) other affilitation established in view of the specificity of the operations or transactions based on the application of the measures under the LMML.

"Senior managing 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 operation or transaction" means any operation or transaction 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 operation 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.

"Actual 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 actual 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 to 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 trust ownership, 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 actual 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.

The actual owner shall not be 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 actual owner is established.

"Control" means control within the meaning of § 1c of the Additional Provisions of the Commercial Act, 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 compositions 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 actual owner in accordance with, or where there is doubt that the person or persons identified is/are not the actual owner/s, the natural person who holds the office of senior managing official shall be deemed to be the "actual owner".

III. CRITERIA FOR IDENTIFYING SUSPICIOUS OPERATIONS AND TRANSACTIONS WITH CLIENTS.

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 of a risk of money laundering and terrorist financing are present.
- Purchasing large packages of financial instruments from clients when the funds invested are not consistent with the information gathered about their financial situation.
- Purchase and sale of large packages of financial instruments in circumstances judged to be unusual and giving rise to a suspicion of a risk of money laundering and terrorist financing.
- Non-cash payment in BGN or foreign currency for the purpose of purchasing financial instruments and a subsequent request to sell what has been acquired and an order to transfer the amounts to an account with a different holder than the one from which the amounts were originally received.
- Non-cash payment in BGN or foreign currency to purchase financial instruments for participation in a privatization transaction and a subsequent request to sell the acquired financial instruments and order the transfer of the amounts to an account with a different holder than the one from which the amounts were originally received or to a branch of a company located in another country.

- Purchases 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 holder or from an account for which there is reason to suspect its use as a "post-box".
- Series of unusual purchase and sale transactions of the same financial instruments by different customers over a short period of time, raising suspicions of a risk of money laundering and terrorist financing.
- 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 a risk of money laundering and terrorist financing.
- Frequent purchases of financial instruments by the same client, where the total amount exceeds BGN 30,000 for a short period of time, and where other circumstances giving rise to suspicion of a risk of money laundering and terrorist financing are present.
- 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 another circumstance that raises a suspicion of improper legitimation or representation is present.
- 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 a risk of money laundering and terrorist financing.
- Remittances from foreign investors for participation in privatization or other transactions with subsequent return of the remittance to banks other than the original banks when the investment is unrealised.
- The use of letters of credit and other methods of commercial payment where the foreign trade documents give rise to suspicions of inauthenticity or where such commercial activity is incompatible with the client's core business.
- 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 of a risk of money laundering and terrorist financing.
- The management funds provided by newly established legal entities are in large amounts which are clearly not in line with the capabilities of the newly established legal entity 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.
- Unwillingness of clients to provide information for identification purposes or the documents they provide when entering into contracts/placing orders raises doubts about their authenticity.
- Representatives or proxies of clients present documents of identity and representative authority whose authenticity raises doubts.
- The client refuses to provide documents for his identification.
- The official identity documents presented by the client lack basic details that would fully identify him.
- The client presents identification documents that appear to be counterfeit.
- The client identifies himself with foreign identity documents, the authenticity of which is difficult to verify and other circumstances that raise reasonable doubt as to his identity are present.
- The signature on the identity document does not correspond to the one provided by the client in connection with the operation or 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 carries out all his contacts with the IP only 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 tries to get close to the IP staff by offering money, gifts or services.
- The client quickly declare his/her funds are "clean" and/or has an unusually good knowledge of AML/CTF 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.
- Persons giving as their own address the address of third parties.
- 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.

(3). The dubious origin of money (property, ownership) are:

- offshore jurisdictions;
- countries not implementing FATF recommendations; countries harbouring banking secrecy.

(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 systems for transmitting funds 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 Art. 98 of the LMML 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 LMML ("National Risk Assessment") and the Supranational Risk Assessment and Recommendations of the European Commission under art. 95, para. 2 of the LMML ("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, para. 1 of the LMML, as well as the results of the Supranational Risk Assessment and the Recommendations of the European Commission under art. 95, para.2 of the LMML.

(4) The risk assessment referred to in this Article shall be carried out by the Executive Directors of the IP and updated every two years.

Client risk assessment

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 actual owner of the client (where applicable); 2. the country or geographical area in which the client or its actual owner is established and the

associated money laundering and terrorism risk; 3. the products and services offered by the IP and the type of transactions carried out on behalf of the client; 4. the delivery mechanisms used for the products, services and transactions referred to in item 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 special and continuous monitoring.

Art. 8. Entering into and continuing business relationships with higher risk clients must be approved by the Executive Directors or a senior IP officer.

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 defined criteria) that may affect the client's assessment;
- in the annual review of higher risk clients.

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

1. High-risk clients. Extended due diligence is applied to high-risk clients.
2. Medium risk clients. Medium risk clients are subject to standard due diligence depending on the client.
3. Low risk clients. Low risk clients are subject to standard due diligence. In the event that the IP undertakes the procedures set out in the LMML and the necessary requirements are met for all or part of the low risk clients, then simplified due diligence should be applied to those clients. In order to avoid confusion between low-risk clients and the verification standard and low-risk clients and the simplified verification standard, text indicating the application of the simplified verification should be added to the risk level of the latter in the IP's systems and documents.

Risk assessment of products, services and delivery mechanisms

Art. 11. All new and existing products, services and transactions offered or carried out by the IP, as well as the delivery mechanisms, shall be assessed 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 Head of the IP Specialist Service shall carry out the risk assessment under this Article. The specific practical steps for risk assessment of product, services and mechanisms shall be specified in a risk matrix prepared by the IP.

Art. 12. Belonging to the lists under Art. 4b of the LMFT

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 actual owner is a person who is included in the lists referred to in Art. 4b of the Law on Measures Against the Financing of Terrorism (LMFT). 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. 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.
(2) The IP shall apply the client due diligence measures when establishing Business relationships;

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

Identifying clients and verifying their identity

Art. 14. (1) When identifying the clients that are natural persons, as well as the representatives and proxies of legal entities, the IB shall collect 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 bears a photograph of the client;
4. any nationality the person holds;
5. country of residence and address (PO Box number is not sufficient).

(2) The IP identifies individuals by requesting an official identity document and taking a copy of it. Where the official identity document does not contain all the data referred

to in items 1 to 5 above, the missing data shall be collected by presenting other official identity documents or other official personal documents that have not expired and bear a photograph of the client and taking a copy thereof. In the absence of any other possibility, the collection of the data referred to in para. 1, item 3 and 5 above may also be carried out by submitting other official documents or documents from a reliable and independent source.

(3) Where, in accordance with the legislation applicable to the IP's activity, identification is carried out without the presence of the natural person to be identified, identification may also be carried out by presenting a copy of an official identity document.

(4) The IP also collects information and data on the professional activity of the person and the purpose of the contract.

Art. 15. (1) When identifying the clients of legal entities IP shall collect data on:

1. name;
2. legal form;
3. domicile;
4. registered address;
5. address for correspondence;
6. current subject of activity and purpose and nature of the business relationship;
7. duration of the undertaking;
8. control bodies, management and representation bodies;
9. type and composition of the collective management body;
10. principal place of business;
11. ownership, management and control structure of the client - a legal person or other legal entity.

(2) With respect to Bulgarian commercial companies and non-profit legal persons, as well as in the case of the existence of an official public commercial or company register in the Member State where the legal person is registered, the identification of legal persons and the collection of data shall be carried out by making a reference to the commercial register or to the relevant public register on the account of the legal person and documenting the actions taken on the identification in accordance with Section IX. In this case, the officer carrying out the verification shall take a printout from the register of all documents containing the data referred to in items 1 to 11, as well as of the general view of the account of the legal person concerned, with data on the date of the last update thereof, and certify the printed documents by affixing his signature, date and time of the verification. The printouts made shall be kept in the client records in the manner specified in Section IX. No printout may be made of the data collected if signed after it has been collected with the official's qualified electronic signature. The documents collected and/or printouts made shall be kept in the client records in the order specified in Section IX. The same shall apply to the reference of client individuals, representatives, proxies and/or actual owners.

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;

(3) In all other cases, the identification of legal persons and other legal entities shall be made by submitting:

- original or notarised copy of an official extract from the relevant register of good standing;
- a copy of the memorandum of association, the articles of incorporation or any other document necessary to establish the data referred to in para. 1, items 1 to 11, certified by the representative;
- a copy of the relevant licence, permit or registration certificate (in case the activity is subject to licensing or permit), certified by the representative.
- Other company documents.

Where the documents do not contain the data referred to in para. 1, items 1 to 11, their collection shall be carried out by submitting other official documents.

Identification of the actual owner

Art. 16. (1) The IP shall identify any natural person who is the actual owner of a client that is 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 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).

(2) The data referred to in para 1, items 1 to 5 above shall be collected by:

1. Reference to the accounts of legal persons 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 good standing, a certified copy of the memorandum of association, the articles of incorporation or any other document necessary to establish the data referred to in para. 1, items 1 to 5;
4. 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 the actual owners of the client, being a body corporate or other legal entity with nominee directors, nominee secretaries or nominee owners of capital;
5. Declaration by the legal representative or proxy of the legal person where the means referred to in items 1 to 4 above have resulted in conflicting information.
6. Other company documents.

(3) For clients that are legal entities whose shares are traded on a regulated market, which are subject to disclosure requirements in accordance with European Union law or

equivalent international standards ensuring an adequate degree of transparency with respect to ownership, the IP shall collect the information on the shareholding subject to disclosure under Chapter Eleven, Section I of the Law on Securities Trading, or similar information concerning companies whose shares are traded on a regulated market outside the Republic of Bulgaria.

Verification of the identification of the client, respectively the actual owner of the client-legal entity

Art. 17. (1) The verification of the data collected under Art. 14 and Art. 16 shall be carried out using one or more of the following methods:

1. requesting additional documents, at the discretion of the IP on a case-by-case basis;
2. confirmation of identification by another person obliged under the LMML or by a person obliged to implement AML measures in another Member State or in a Reliable third country;
3. consulting electronic websites and databases of domestic and foreign competent state and other authorities made available for public use for the purpose of verifying the validity of identity documents and other personal documents or verifying other data collected in the course of identification;
4. making enquiries in publicly available local and foreign official commercial, company, corporate and other registers;
5. use of technical means to verify the authenticity of the documents submitted;
6. establishing a requirement that the first payment under the operation or transaction be made through an account opened in the name of the client with a credit institution in the Republic of Bulgaria, in another Member State or with a bank in a Reliable third country;
7. re-request of the documents presented at the time of identification and verification of any change in the identification data - when verifying the identification in the course of an established business relationship, where the identification was made at the time of entering into such a relationship;
8. establishing a requirement that all payments under the operation or transaction are made by the client through a payment service provider from the Republic of Bulgaria, an obliged person under art. 4(2) of MAMLA, or from another Member State or a bank from a Reliable third country that also applies the measures provided for in Directive (EU) 2015/849;

(2) In the case of remote conclusion of contracts in connection with the IP Activity without the presence of the client, the verification of the collected identification data shall be carried out by at least two of the means specified in items 1 to 8.

(3) The action taken shall be documented by the official carrying out the check to verify the data by affixing his/her signnature, date, time, names and position on the documents collected. In cases where the verification is carried out through electronic databases, the official shall take a printout containing the relevant data and shall place signature, date, time, names and position on the printout. A printout may not be made of the data collected if it is signed after it has been collected with the official's qualified electronic signature. The

documents collected and printouts taken shall be kept in the client record in the order specified in Section IX.

Reference to previous identification

Reference to previous identification by a credit institution:

Art. 18. The IP may rely on a previous identification of the client, respectively its actual owner, made by a credit institution, provided that the following cumulative conditions are met:

1. the domicile of the credit institution that carried out the identification is in the Republic of Bulgaria, in another Member State or in a Reliable third country; 2. The data to be collected from the IP under Art. 14, 15 and 16 of this Section shall be available to the IP and copies thereof shall be immediately available upon request;

3. upon request, the credit institution that has carried out the previous identification shall be able to provide within three days to the IP certified copies of the documents referred to in item 2.

Reference to previous identification within the group:

Art. 19. IP may rely on prior identification of the client, or his/her actual 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 applies client due diligence measures, rules on record keeping and AML/CTF programmes in accordance with the LMML;

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. 20. (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. 14 et seq. above and subject to the requirements of Art. 59 of Regulation No. 38.

(2) Where it is suspected 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 the notification referred to in Art. 35 below 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 actual owner;

4. requires additional documents;

5. makes inquiries in publicly accessible local and foreign official commercial, company and other registers;

6. consult publicly available sources of information;

7. exchange information within the group;

8. requires confirmation of identification from another person obliged under the LMML or from a person obliged to implement AML measures in another Member State or in a Reliable third country;

Clarification of the origin of funds

Art. 21. (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 his/her main activity, including the actual and expected volume of business and the operations or transactions expected to be conducted within that relationship, by completing a client 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 LMML 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 para. 1, and in cases where the application of at least two of the means under para. 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. The clarification of the origin of the funds may be made by a written declaration in a form by the client or his/her legal representative or proxy where the application of two of the means referred to in para. 1 has been inconsistent.

Gathering information and assessing the purpose and nature of the business relationship that has been established or is to be established with the client

Art. 22. When entering into a business relationship with a client, the IP shall collect data on the person's professional activities and the purpose and nature of the person's involvement in the business relationship by using documents, data or information from a reliable and independent source, completing a questionnaire or in any other appropriate manner.

Ongoing monitoring

Art. 23. 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 identify in a timely manner the existence of any of the risk factors referred to in Section IV above, and to take the necessary measures to prevent and manage the risks of money laundering and terrorist financing in these cases.

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

General measures for enhanced due diligence

Art. 24. (1) The IP shall apply general enhanced due diligence measures, together with the measures referred to in item 1 of this section, in all cases where, taking into account the factors referred to in section IV, it has identified a high level of risk, and in addition to the specific enhanced due diligence measures referred to in Art. 25 et seq. below, where their application is not sufficient to mitigate the identified risks of money laundering and terrorist financing.

(2) The IB 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 item 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 Specialised Service 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 LMML;
7. commissioning of investigations or other actions necessary for this purpose to persons of good repute and proven expertise and practical experience in the prevention and suppression of money laundering and terrorist financing;

Specific measures for enhanced due diligence

Art. 25. The IP shall apply specific measures for enhanced due diligence in addition to and together with the measures under Art. 24.

Measures when concluding a contract with promenient political figures or persons associated with promenient political figures

(1) Contracting with clients who are promenient political figures (PPF) or persons associated with promenient political figures, including clients whose actual owner is a PPF or a person associated with a PPF, requires the approval of the ***IP's executive officers or a senior officer***. In cases where, after entering into a contract with a client, it is determined that the client or its actual owner is a PPF or a person associated with a PPF, the continuation of the business relationship with that client may only take place after approval by the ***IP's executive directors or a senior officer***.

(2) The IP shall establish, in accordance with these Rules, the ***origin of the funds*** used in the business relationship and the transactions and operations carried out on the basis of a contract concluded with a client who is a PPF or a person related to a PPF or whose actual owner is a PPF or a person related to a PPF.

(3) The IP shall take appropriate action to clarify the ***source of the assets*** of a client or actual owner of a client, a PPF or a person associated with a PPF by periodically reviewing and comparing the information about the declared assets of the client or actual owner of the client with the information established as a result of the application of the due diligence measures.

(4) The IP shall conduct ***ongoing and enhanced monitoring of its business relationship*** with a client that is a PPF or a PPF's affiliate, or whose actual owner is a PPF or a PPF'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 operations that could affect the level of identified risk.

(5) The IP introduces a requirement for approval of the ***IB's executive directors or a senior official*** to continue a business relationship with a client where, in the course of ongoing and enhanced monitoring of a business relationship with a client who is a PPF or a PPF-related person or whose actual owner is a PPF or a PPF-related person, potentially higher risk situations are identified.

(6) The actions of the IP under para. 3 and 4 shall be documented and updated on an annual basis. The update shall be carried out twice a year where the client or the actual owner of the client is from a country for which information on an identified high level of corruption or on identified significant gaps in the AML/CFT enforcement mechanisms is present or where the client or the actual owner of the client is linked to a sector for which the Supranational Risk Assessment, the National Risk Assessment or the Risk Assessment under Section IV of these Rules has identified a higher risk of corruption or money laundering.

(7) The measures referred to in this Article shall not apply in the event that the client, respectively his/her actual owner, has ceased to hold the office, which served as the basis for his designation as a promenient political figure 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 whether one or more of the enhanced due diligence measures should be continued. The assessment shall be documented and maintained in accordance with Section IX and updated on an annual basis.

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

Art. 26. Where complex or unusually large transactions and 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 and operations:

1. Ongoing and enhanced monitoring of all complex or unusually large transactions and 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 transactions and operations, relevant documents and other identifying data. The IP shall document its assessment as to the existence of the conditions for reporting under Art. 72 of the LMML as a result of the information collected.

Determination of measures for enhanced due diligence

Art. 27. 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 triggering the application of the enhanced due diligence measures and shall store the collected data, documents and information in accordance with Section IX.

Simplified due diligence

Art. 28. The IP may apply simplified due diligence measures subject to the conditions and in accordance with the procedure provided for in the LMML and the RILMML.

Additional restrictions on the IB Activity

Art. 29. In the course of the IP Activity:

1. According to the current regulations applicable to the activity of the IP, the same may not act on behalf of a client without having identified the client in advance. Therefore, it is not allowed to anonymously carry out transactions and operations 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 should limit payments (client deposits and withdrawals) in cash, making such payments only exceptionally. Examples of cases where exceptions may be allowed are:

- a withdrawal from a client where that client does not have a bank account;
- in the case of a client making a small non-regular transactions and wishing to withdraw a small amount of cash;
- when a client deposits a small amount necessary to pay commissions owed to the IP;

In any case of an exception, the cash payment must comply with applicable law and be approved by both Executive Directors.

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. INTERNAL SYSTEM FOR ESTABLISHING WHETHER THE CLIENT OR ITS ACTUAL OWNER IS PROMENIENT POLITICAL FIGURE OR A PERSON ASSOCIATED WITH A PROMENIENT POLITICAL FIGURE

Art. 30. (1) When concluding a contract in connection with the IP's Activity, the IP shall use at least one of the following means to establish whether the client, respectively its actual owner, is a promenient political figure or a person related to a promenient political figure:

1. using information obtained through the application of the enhanced due diligence measures;
2. requiring the client to make a written declaration to establish whether the person falls within any of the categories set out in Art. 36 of the LMML.
3. consult internal or external databases (Worldcheck, https://namescan.io/FreePEPCheck.aspx; https://www.keesingtechnologies.com/)

(2) IP shall use at least two of the above means to determine whether the client or its owner is a PPF when:

1. the client or the actual owner of the client is from a country where information of high levels of corruption is present, 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 that is legal person or other legal entity, has an ownership structure that includes nominee owners and managers or otherwise makes it difficult to identify the actual 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. where a higher risk has been identified under Section IV and Section V of these Rules.

(3) Where the IP determines that the client or his/her actual owner is a PPF, it shall apply the specific enhanced due diligence measures in Art. 25 of these Rules in addition to the due diligence measures in Section V (1) above. In the event that the above measures are not sufficient to mitigate the money laundering and terrorist financing risks identified by the IP, the IP shall apply the general enhanced due diligence measures referred to in Art. 23 of the Rules in addition to the measures referred to in the preceding sentence.

VII. USE OF TECHNICAL MEANS TO PREVENT AND DETECT MONEY LAUNDERING. INTERNAL CONTROL SYSTEM FOR REMOTE, DEFAULT CONCLUSION OF CONTRACTS WITH CLIENTS.

Art. 31. (1) When remotely concluding contracts and providing services, the IP shall, subject to the requirements of Regulation No 38, use technical means for the prevention and detection of money laundering in cases where there are doubts as to the reliable identification of the client or his/her actual owner. The technical means used by the IB are intended to prevent:

1. provision of false identification data by the identifiable natural person;
2. the use of foreign identification and identity documents;
3. providing identification and proof of identity under threat, coercion or other similar circumstances.

(2) IP shall verify the identity documents provided remotely and, in case of doubt, those presented when meeting with a client in:

- Database maintained by the Council of the European Union - https://www.consilium.europa.eu/prado/en/check-document-numbers.html or https://www.keesingtechnologies.com/ ;
- The database maintained by the Ministry of Interior - https://www.mvr.bg/електронниуслуги/електронни-услуги-и-справки/справка-за-валидност-на-български-личнидокументи .
- Other similar databases maintained by official bodies of other countries.

(3) In case of remote conclusion of a contract in the cases referred to in Art. 32, paragraphs 2-4 for the provision of Investment and/or Ancillary Services, the IP shall establish additional measures aimed at ensuring the possibility of:

1. identification of changes or damage to security features and their location in identity documents;
2. comparing the security features of the identity documents with those of the predefined ones in an internal template database or in reliable external template databases;
3. locating the identifiable person;
4. clarifying the reasons why a client from another country or jurisdiction is using the services of the IP;
5. applying restrictions on the documents accepted by applying at least two of the following requirements:

a) acceptance only of official identity documents containing protective elements;

(b) acceptance only of official identity documents containing biometric data;

(c) requirement to use a qualified electronic signature;

(d) requirement for notarisation of the contract;

(e) requirement to provide a document (reference or statement of account) issued by a bank or licensed payment institution;

(f) requirement that the first payment into a client's account be made from the client's own payment account opened with a bank or payment institution that applies similar AML/CTF measures.

6. use of traditional methods of communication, e.g. sending a letter to the address of the client indicated in the identity document, making a telephone call, exchanging electronic messages by e-mail indicated by the client;

(4) In the event that the verification of the identification under para. 3 proves to be insufficient for the purposes of mitigating the risks of money laundering or terrorist financing, the IP may arrange a video conference with the person to be identified. The video conference shall meet the following conditions:

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

(5) At the discretion of the person exercising internal control over the fulfilment of the obligations of the LMML and the RILMML, the IB may use other technical means to verify the authenticity and reliability of the identity documents provided by the client, respectively his/her representative, when concluding contracts in connection with the activities of the IP.

Art. 32 (1) In case of default conclusion of a contract for the provision of Investment and/or Ancillary Services, the IP shall establish a methodology and steps for the conclusion of a contract. These shall be adopted by the Head of the Specialised Service referred to in art. 106 of the LMML and may be supplemented and updated at his/her discretion.

(2) The contract referred to in para. 1 may be concluded remotely by exchange of the necessary documents signed by the parties in accordance with the requirements of Art. 55, para. 2 of the LMML.

Verification of the identification of natural person clients or the representative and ultimate actual owners of legal person clients shall be carried out by applying at least 2 of the methods below:

1. requesting additional documents;
2. confirmation of the identification by another person referred to in Art. 4 or by a person obliged to apply AML measures in another Member State or in a third country referred to in Art. 27;
3. consulting electronic websites and databases of domestic and foreign competent state and other authorities made available for public use for the purpose of verifying the validity of

identity documents and other personal documents or verifying other data collected in the course of identification;

4. making enquiries in publicly available local and foreign official commercial, company, corporate and other registers;
5. use of technical means to verify the authenticity of the documents submitted;
6. establishing a requirement for the first payment under the transaction or operation to be made through an account opened in the name of the client with a credit institution from the Republic of Bulgaria, from another Member State or from a bank from a third country under Art. 27;
7. re-request of the documents presented at the time of identification and verification of any change in the identification data - when verifying the identification in the course of an established business relationship, where the identification was made at the time of entering into such a relationship;
8. any other means which gives reason to the person referred to in Art. 4 to believe that the identification of the client is reliable.

The Head of the Specialised Service under Art. 106 of the LMML shall issue and maintain up-to-date prescriptions and clarifications on which methods to apply in the case of clients from certain countries, as well as on the specific application of the methods under item 1 and 8 above.

(3) Records shall be maintained in the general order of all documents and records maintained in the IP in accordance with the Record Keeping Rules. The documents received in electronic form along with the contract accepted by the client and given a unique number along with the declarations and other documents additionally required shall be stored in an electronic file and/or on paper, and the electronic messages sent and received shall be stored electronically.

VIII. SPECIALISED SERVICE. INTERNAL CONTROL SYSTEM

Art. 33 (1) The IP shall establish a specialised service under Art. 106 of the LMML, designated by order of the governing body, which shall prepare, propose for approval, and implement training programs for employees on the application of the LMML, its implementing acts, and these Rules, and shall organize, manage, and control the activities of:

1. collecting, processing, storing and disclosing information about specific transactions or operations;
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 transactions or operations and on the source of the assets;
4. collecting information on clients and maintaining accurate and detailed records of their operations in cash or valuables, including the information and documents referred to in Art. 6 of the Foreign Exchange Act;
5. providing the collected information to the Financial Intelligence Directorate of the State Agency for National Security.
6. The system for internal control over the fulfilment of obligations under the LMML is based on (and documented through) the completion of checklists.

(3) On appointment of a new employee, a checklist as per Annex II shall be filled;

(4) For the purpose of carrying out annual internal control over the implementation of the obligations under the LMML, a checklist in accordance with Annex III shall be completed within the time limits referred to in Art. 55.
(5) The Specialised Service shall be headed by the Executive Director of the Company, who shall be responsible for the internal control of the implementation of the obligations under the LMML, the RILMML and these Rules. The Head shall be appointed by order of the IP's governing body.

(6) The IP may establish a specialised service under the conditions and in accordance with the procedure of Art. 106 of the LMML 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 LMML, notify the Financial Intelligence Directorate of the State Agency for National Security of the name of the officer, as well as provide contact details for the officer.

IX. INTERNAL AUDIT

Art. 34 (1) The Internal Audit Unit in the IP shall carry out verification and evaluation of:
1. policies and procedures on AML/CTF measures;
2. due diligence and enhanced due diligence checks carried out and the methods of implementation;
3. monitoring of transactions carried out;
4. transaction tracking performed;
5. trainings conducted;
6. existence of reports of suspicious activity, the documents collected and the action taken;
7. institution's risk assessment and client risk assessments;
8. inspections and assessment of compliance by the IP and individual employees with their obligations under the LMML, the RILMML and these Rules.

(2) The Internal Audit Unit of the IP shall include in its plan to carry out inspections and assessments of compliance by the IP and individual staff members with their obligations under the LMML, the RILMML and these Rules.
(3) Upon completion of the review, the Head of Internal Audit Unit may make recommendations to remedy any non-compliance identified. In the cases referred to in the preceding sentence, the department shall verify the actions taken and measures implemented in accordance with the recommendations and certify their implementation.
(4) The Internal Audit Unit shall include in the report to the Board of Directors of the IP information on the non-compliances identified in the framework of the controls referred to in para. 1 and the measures taken to remedy them.

X. PRESERVATION AND DISCLOSURE OF INFORMATION. REVIEW AND UPDATE OF THE DATABASE

Record keeping

Art. 35 The IP shall keep all documents, data and information collected and prepared under these Rules for a period of 5 years from:

1. the beginning of the calendar year following the year of termination of the relationship with the client in respect of documents prepared and received in connection with established business relationships with clients.
2. from the beginning of the calendar year following the year of disclosure of the information in cases of disclosure of information under Art. 35 of this Section
3. from the beginning of the calendar year following the year of their preparation for documents prepared in connection with the Risk Assessment under Section IV and V.

(2)Upon written instruction of the Director of the Financial Intelligence Directorate of the State Agency for National Security, 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 Agency for National Security, the relevant supervisory authorities and the auditors. The documents, information and data shall be made available to the Financial Intelligence Directorate of the State Agency for National Security 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. 36 (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 Agency for National Security, prior to carrying out the relevant operation or transactions, by delaying its implementation within the time limit allowed under the regulations governing the relevant type of activity.

(2)In the notification under para. 1, the IP shall specify the maximum period within which the operation or transaction may be postponed.

(3)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 Agency for National Security.

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

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

Disclosure of other information

Art. 37 At the time of preparation of these Rules, the IP has restricted payments (client deposits and withdrawals) in cash, making such payments only on an exceptional basis. The cases in which exceptions may be made are described in Article 29(2) of these Rules.

(2) In the event that in the future the IP adopts an amendment to its Internal Rules and accepts payments in cash, the IP shall notify the Financial Intelligence Directorate of the State Agency for National Security of any cash payment in excess of BGN 30 000 or their equivalent in foreign currency, made by or to its client within the established relationship, by the 15th day of the month following the month to which the information relates, on paper or magnetic media or electronically in a form approved by the Director of the Financial Intelligence Directorate of the State Agency for National Security.

Register

Art. 38 (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 maintained in an electronic form that meets the following requirements:

1. its functional characteristics allow:
   (a) verifying the time of recording of the message to the nearest year, date, hour, minute and second with a qualified time certificate;
   (b) creation of a historical record of all movements related to the introduction of electronic register entries;
2. its functional characteristics do not allow:
   (a) changing the order of recorded messages or their content;
   (b) unlawful destruction and/or deletion of a recorded message;

(c) unauthorised access, alteration or distribution of the register.

(3) The person designated to exercise internal control over the performance of the obligations under the LMML and its implementing regulations shall be responsible for the proper maintenance and preservation of the register. When a communication is made in the register, the person to whom the communication is made shall open a file in which all documents relevant to the actions carried out by the IP's employees related to the communication made on suspicion of money laundering, respectively to the relevant complex or unusually large operations and transactions, shall be collected and arranged in the order of their receipt.

Updating the databases

Art. 39 (1) The IP shall keep up-to-date the information about its clients and the operations and transactions carried out by them, periodically reviewing and updating, if necessary, the databases and client files maintained. The review referred to in the preceding sentence shall be carried out as follows:

Client risk profile	Periodicity
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 operations or transactions are carried out;
3. IP becomes aware that the information it has on an existing client is insufficient for the purposes of applying the due diligence measures;
4. 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. 40 (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 operations and transactions and the nature and purpose of the established business relationship and/or the risk identified in relation to the business relationship with the client.

XI. ALLOCATION OF RESPONSIBILITIES

Art. 41 The overall responsibility for the performance of the obligations of the IP in accordance with the LMML, the RILMML and these Rules shall be borne by the Board of Directors of the IP.

1. IP Board of Directors:

- Accepts these Rules
- Appoint and dismiss the Head of the Specialised Service and the person discharging the duties under the LMML for the branch of the Intermediary.
- Provide overall supervision and guidance in relation to the IP's compliance with its obligations under the LMML, the RILMML 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 Art. 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 level of risk identified 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/some of the criteria for suspicious operations and transactions 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/some of the criteria for suspicious operations and transactions in relation to the investment services and activities carried out by the IP.

XII. EMPLOYEE TRAINING

Art. 42 (1) The IP shall provide for the conduct of induction, ongoing (continuing) and specialised (ad hoc) training, in respect of the Specialised Service and other IP staff, under the conditions and within the timeframes specified 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 AML 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 Agency for National Security.

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 employees' employment record.

XII. INTERNAL SIGNALS

Art. 43 Any employee of the IB may lodge an alert, including anonymously, in case of suspicion of money laundering, to the person who implements the internal control on the implementation of the obligations under the LMML and the implementing rules of the IP at the address of the management of the IP. The IP shall guarantee the anonymity of the employees who have lodged alerts under the previous sentence.

(2) The Head of the Specialised Service shall immediately record the alert received in the register referred to in Art. 38 above.

The Head of the Specialised Service shall immediately examine the alert received, make the necessary assessment of the case and, if necessary, make a notification in accordance with Art. 36 above. The verification by the person exercising internal control of the fulfilment of the obligations under the LMML and its implementing rules and the assessment made shall be documented and kept in accordance with Section IX of these Rules.

XIII. FINAL PROVISIONS

§1. These Internal Rules have been adopted by a resolution of the Board of Directors of IP dated 31 March 2021 and repeal the previous ones adopted on 29 January 2021.
§2 The Rules shall be subject to annual review by the Head of Specialist 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 Intermediary in the country and abroad.

ANNEXES:

ANNEX I – INDICATIVE TABLE FOR DETERMINING THE CLIENT RISK PROFILE
ANNEX II – CHECKLIST FOR NEW EMPLOYEES
ANNEX III – CHECKLIST OF ANNUAL INTERNAL CONTROL

ANNEX IV – REPORTING ON SUPRANATIONAL AND NATIONAL RISK ASSESSMENT

Annex I

I. Risks associated with the client/ actual owner of the client			
1. Economic activity of the client/ actual owner of the client			
Factor	Business relationship with the client	Level of risk	Measures to be implemented by IB[1]
Corruption-related sectors	No	Medium	I
	Yes	High	I, II
Money laundering-related sectors	No	Medium	I
	Yes	High	I, II
Cash payments-related sectors	No	Medium	I
	Yes	High	I, II
2. Purpose and activity of the client – legal entity			
Asset management	No	Medium	I
	Yes	High	I, II
Non-profit organization supporting high-risk jurisdictions	No	Medium	I
	Yes	High	I, II
New company without appropriate profile and business results	No	Medium	I
	Yes	High	I, II
Special purpose vehicle	No	Medium	I
	Yes	High	I, II
	No	Medium	I

Third country special purpose vehicle	Yes	High	I, II
Prominent political figure or a person associated with a prominent political figure	No	Medium	I
	Yes	High	I, II, III
Person holding an important position	No	Medium	I
	Yes	High	I, II, III
Legal entity for which legal requirements for disclosure exists	No	Medium	I
	Yes	Low	I
Discrepancy between collected and available client information	No	Medium	I
	Yes	High	I, II

Belonging to the lists referred to in Article 4b of LMFT	No	Medium	I
	Yes	Unacceptable	IB refuses to conclude a contract
Unusual, complex, opaque ownership structure	No	Medium	I
	Yes	High	I, II
Bearer shares	No	Medium	I
	Yes	High	I, II
Nominee company with unknown shareholders	No	Medium	I
	Yes	High	I, II
Institutional investor whose status has been verified by a government agency from EEC	No	Medium	I
	Yes	High	I

Government body from EEC jurisdiction	No	Medium	I
	Yes	High	I
Financial institution established in a jurisdiction from EEC	No	Medium	I
	Yes	High	I
3. Reputation of the client/actual owner of the client			
Information on indictments of terrorism	No	Medium	I
	Yes	Unacceptable	IB refuses to conclude a contract
Indictments or suspicion of criminal activity	No	Medium	I
	Yes	Unacceptable	IB refuses to conclude a contract
Previous notifications under Article 72 of the LMML	No	Medium	I
	Yes	Unacceptable	IB refuses to conclude a contract
4. Behaviour of the client/actual owner of the client			
Unwillingness to identify	No	Medium	I
	Yes	High	I, II
Avoiding the conclusion of contract	No	Medium	I
	Yes	High	I, II
Willingness to conclude remotely or anonymously contract without good reason	No	Medium	I
	Yes	High	I, II

Lack of economic and legal logic of the operations carried out	No	Medium	I
	Yes	High	I, II, IV
	No	Medium	I

Unusual scheme, justification of transactions and operations	Yes	High	I, II, IV
Unusual and/or complex and/or unexpectedly high volume operations	No	Medium	I
	Yes	High	I, II, IV
Pursuit for excessive privacy	No	Medium	I
	Yes	High	I, II
Discrepancy between established origin of funds/property and available information	No	Medium	I
	Yes	High	I, II
Lack of reason for a client from another country to uses the IP services	No	Medium	I
	Yes	High	I, II
Lack of economic purpose of the investment	No	Medium	I
	Yes	High	I, II, IV
Early exit from a long-term investment with risk of loss	No	Medium	I
	Yes	High	I, II
Multiple purchases and sales in a short period of time without economic justification	No	Medium	I
	Yes	High	I, II
Frequent changes in information about the client	No	Medium	I
	Yes	High	I, II
Using multiple accounts	No	Medium	I
	Yes	High	I, II
Involvement of multiple parties in transactions, incl. Nominee companies	No	Medium	I
	Yes	High	I, II

I. Countries and geographical areas in which the client or its actual owner is established			
States included in the list referred to in Article 46, para. 3 of LMML	No	Medium	I
	Yes	High	I, II

Instructions issued by the Financial Intelligence Directorate	No	Medium	I
	Yes	High	I, II
Information in the media that the State does not have effective countermeasure systems	No	Medium	I
	Yes	High	I, II
Sanctions and embargoes imposed by the European Parliament, the Council or the Security Council of UN	No	Medium	I
	Yes	High	I, II
Non-compliance with international tax standards	No	Medium	I
	Yes	High	I, II
No register of actual owners	No	Medium	I
	Yes	High	I, II
Availability of information on high levels of corruption, tax crimes, organized crime	No	Medium	I
	Yes	High	I, II
II. Services offered			
Unusually large operations	No	Medium	I
	Yes	High	I, II
Possible payments to a third party	No	Medium	I
	Yes	High	I, II
	No	Medium	I

Involvement of many persons from different jurisdictions	Yes	High	I, II
Unusual payments from third parties	No	Medium	I
	Yes	High	I, II
Payments from third parties that cannot be identified	No	Medium	I
	Yes	High	I, II
Transfer of client funds to a non-controlled institution	No	Medium	I
	Yes	High	I, II
III. Delivery mechanisms			
Previous identification by tied agent	No	Medium	I
	Yes	High	I, II
Previous identification by a person in the group	No	Medium	I
	Yes	High	I, II
Previous identification by a Reliable third party credit institution	No	Medium	I
	Yes	High	I, II
Remote conclusion of a contract with an ordinary electronic signature	No	Medium	I
	Yes	High	I, II, V

Annex II

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 LMML, the RILMML, the LMFT, the internal rules under the LMML 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 III

CHECKLIST OF ANNUAL INTERNAL CONTROL

IN THE ANNUAL INTERNAL CONTROL ON THE IMPLEMENTATION OF THE OBLIGATIONS UNDER LMML FOR 2020 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 CONNECTION WITH THE 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 actual owner of, a prominent political figure or a person associated with such a figure (a person referred to in Article 36 of the LMML) - [ ] No [ ] Yes: ..... number of business relationships

E. Relationship review and risk reporting performed on clients and actual owners of clients who have been identified as persons under Article 36 of the LMML 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 IV

CONSIDERATION OF SUPRANATIONAL AND NATIONAL RISK ASSESSMENT

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

1. Supranational risk assessment

The SRA of ML/TF 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 SRA 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 June 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 July 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 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 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

[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 .

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 SRA

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

2. National risk assessment

2.1. Summary of the NRA

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

In the summary of the NRA, SANS 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 SANS 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. 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,

[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 .

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 LMML 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 LMML below.