ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING INTERNAL COMPLIANCE POLICY

of

OPEN FINTECH SOLUTIONS SRL

Last revision on: 01.09.2023

Index

1. INTRODUCTION

This document summarizes the legal and regulatory framework which Open Fintech Solutions SRL (hereinafter referred to as "**OFS**") will observe in the conduct of their business activity. In addition, this document is designed to provide a system of risk-based controls in order to facilitate, thorough due diligence, the identification, mitigation and management of anti-money laundering and counter-terrorist financing threats (hereinafter collectively referred to as "**ML**" - Money Laundering - respectively "**TF**" Terrorism Financing)

1.1 OFS's internal compliance procedures and rules include the following goals:

(a) performing the know your client procedures (hereinafter "**Customer Due Diligence**" or "**CDD**") which encompass the identification and verification of direct customers, business partners, ultimate beneficial owners thereof and/or politically exposed persons ("**PEP**"), according to the Know Your Customer/Business requirements ("**KYC**" or "**KYB**"), throughout the on-boarding phase as well as during the entire contractual relationship, through continuous oversight of our direct customers or business partners;

(b) Designating the person responsible for the fruition of the legal requirements related to anti-money laundering and counter-terrorism financing - a Conformity Officer for the purposes of article 23 para. (2) from Law 129/2019 , appointed at a management level, having the duties provided by law for ensuring the conformity of OFS's internal policies, norms and internal measures (hereinafter "**Conformity Officer**" or "**MLRO**" - Money Laundering Reporting Officer);

(c) Setting processes for screening employees and customers;

(d) Training the personnel in anti-money laundering and counter-terrorist financing procedures;

(e) Implementing risk-based customer due diligence policies, procedures, and processes that are compliant with applicable regulations and legislation;

(f) Identifying suspicious transactions and taking appropriate actions, reporting them internally and submitting such reports in a timely manner, including but not limited to suspicious activity reports (hereinafter "**Suspicious Reports**" or "**SARs**"). Initiating further investigations and subsequently reporting such suspicious activities or breaches to the appropriate regulatory authorities;

(g) Keeping the abovementioned documents and records for the time period set by the applicable law;

(h) Ensuring control and monitoring mechanisms that are adequate for timely detection, investigation and reporting of suspicious activities/transactions.

(i) Prohibiting certain business relationship patterns and activities, including:

i. anonymous accounts;

ii. contracting with fictitious clients (companies or natural persons);

iii. any commercial activity, respectively commencing or pursuing customer relations or provision of services that are considered by OFS to be in potential breach of the applicable laws, including in connection with any commercial activity with natural or legal persons who (a) are indicated on

an official OFAC sanctions list, or (b) reside or are domiciled in the countries or territories currently subject to these sanctions.

It is the Conformity Officer's duty to monitor the compliance of all the policies related to the identification, mitigation and management of ML and FT threats (hereinafter collectively referred to as the "AML Internal Policy").

OFS Personnel are responsible for understanding and implementing the provisions of this policy and for confirming in writing that they have read and understood the provisions of this AML Internal Policy. All OFS personnel (including new employees) is required to undertake AML training within 3 months of starting their employment with OFS and thereafter undertake annual training in line with this policy.

If OFS personnel do not comply with the requirements set out in this policy, this will be considered a material breach of contractual obligations and may lead to disciplinary proceedings.

This Internal AML Policy also constitutes a guide for OFS employees, company management, contractors, MPs, and other third parties with which OFS has business relations.

This document may be subject to changes or completions, as required for operational, business or legislative reasons.

2. TERMS AND DEFINITIONS

Property means assets of any kind, whether tangible or intangible, movable or immovable, as well as legal documents or instruments in any form, including electronic or digital form, attesting to a title or right or interests in respect thereof; (art. 2 letter c of Law 129/2019)

Senior management means any person who has sufficient knowledge of the entity's exposure to money laundering and terrorism financing risk, and who has a sufficiently high ranking to make decisions with effect on that exposure, without the need to necessarily be a member of the collective management and administration body; (art. 2 letter o, of Law 129/2019)

Terrorist financing involves dealing with money or property that you have reasonable cause to suspect may be used for terrorism. The funds and property can be obtained from legitimate or criminal sources and may consist in small amounts.

Virtual Currency *means* a digital representation of value which is not issued or guaranteed by any central bank or a public authority, is not necessarily linked to a legally established currency and does not have the legal status of currency or money, but it is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

From a regulatory perspective, the definition of the terrorist financing offence - in addition to the punishment provided for by law - is set forth in **art. 36 of Law No. 535/2004** *on the prevention and combating of terrorism, as well as for the amendment and completion of certain normative acts*, as follows:

(a) It is a terrorism financing offence, to collect or make available funds, directly or indirectly, whether of lawful or illicit source, with the intention of being used or with knowledge that they are used, in full or in part, for committing acts of terrorism or for supporting a terrorist entity, and it is punishable by 5 to 12 years of imprisonment and the suppression of certain rights.

(b) A criminal offense committed for the purpose of obtaining funds, with the intention of being used or with knowledge that they are used, in full or in part, for committing acts of terrorism or for supporting terrorist entities, is deemed criminal offense and is punishable by law with imprisonment.

Compliance Officer (or MLRO) is the AML central figure within the company responsible for overseeing all the activities related to the matter of financial crime.

Criminal property is deemed to be the proceeds of criminal conduct. This includes but it is not limited to any type of conduct, wherever it takes place, which would constitute a criminal offence in Romania or wherever the offender is located, includes drug and human trafficking, terrorist activity, tax evasion, corruption, fraud, forgery, theft, counterfeiting, smuggling and extortion. This also includes any other offence that is committed for profit.

International limitations *means the restrictions and obligations in relation to the governments of certain states, non-state entities or natural or legal persons, adopted by the United Nations Security Council, the European Union, other international organizations or by unilateral decisions of Romania or other states, for the purposes of maintaining international peace and security, preventing and combating terrorism, ensuring respect for human rights and fundamental freedoms, developing and consolidating democracy and the rule of law and fulfilling other purposes in accordance with the objectives of the international community, the international law and the European Union law.* (art. 2 letter a of GEO 202/2008 on the implementation of international sanctions).

Financial sanctions are measures imposed by national governmental and multinational bodies which seek to alter the behaviour and decisions of other national governments or non-state actors that may threaten the security of the global community or violate international norms of behaviour.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of proceeds derived from crimes so that the unlawful proceeds appear to have legitimate origins or constitute legitimate assets.

From a regulatory point of view, the definition of money laundering offense as well as the punishment levels - are provided in Law 129/2019 on the prevention and countering of money laundering and terrorism financing, as well as for amending and supplementing certain normative acts („**Law 129/2019**”), as follows:

As per. art. 49 of Law 129/2019, the following, constitute money laundering offense and are punishable by 3 to 10 years of imprisonment:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illicit origin of the Property or for the purpose of assisting the person who committed the offence from which the property derives to evade criminal prosecution, trial or serving the sentence;

(b) the concealment or disguise of the true nature, source, location, disposition, movement rights with respect to, or ownership of, Property, knowing that such Property is derived from criminal activity;

(c) the acquisition, possession, or use of Property by a person other than the principal of the offence from which the Property derives, knowing that such Property derives from criminal activity.

(1) The attempt is punishable.

(2) If the act was committed by a legal person, in addition to the criminal fine, the competent court, shall apply also one or more of the supplementary penalties provided for in art. 136 para. (3) letters a)-c) of Law No. 286/2009 regarding the criminal code.

(3) The provisions of para. (1) - (4) apply regardless of whether the offense from which the property originates has been committed in Romania, in other member states or a third state outside the European Union.

Money laundering commonly occurs in three stages:

(a) **Placement**: Cash generated from criminal activities is converted into monetary instruments, such as money or money equivalents (including virtual currencies) or travellers' checks, or deposited into accounts at financial institutions or in crypto wallets.

(b) **Layering**: Funds/virtual assets are transferred or moved into other accounts/virtual wallets or other financial institutions to further separate the money from its criminal origin.

(c) **Integration**: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

3. ABBREVIATIONS:

AML Anti-money laundering

ML Money Laundering

TF Terrorist Financing

GDPR General Data Protection Regulation

KYB Know Your Business

KYC Know Your Client

CDD Customer Due Diligence

EDD Enhanced Due diligence

UBO Ultimate Beneficial Owner

MLR Money Laundering Regulations

MLRO Money Laundering Reporting Officer

SRI National Intelligence Service

PEP Politically Exposed Persons

STR Suspicious Transaction Report

DIICOT Department of Terrorism and Organized Crime Investigation

NOPCML The National Office for Prevention and Control of Money Laundering

BNR The National Bank of Romania

NAFA The National Agency for Fiscal Administration

4. ANTI-MONEY LAUNDERING REGULATIONS (MLR)

References to money laundering regulations (referred to as "**MLR**" – money laundering regulations) reflect at least, but not limited to the provisions of Law No 129/2019;

MLR requires the relevant entities to:

(a) have policies and procedures to prevent their use for money laundering purposes;

(b) have employees trained in such procedures and in the anti-money laundering legislation;

(c) have in place checks and controls to ensure that such policies and procedures are functioning;

(d) Have in place internal and external policies pertaining to the procedures related to suspicious transactions reporting.

Penalties: Criminal conviction under Law 129/2019 may result in fines and/or imprisonment for up to 10 years and the restriction of certain rights.

For the purposes of art. 5 of Law 129/2019, the reporting entities are:

(a) credit institutions;

(b) financial institutions;

(c) private pension fund managers[1];

(d) providers of gambling services;

(e) auditors, insolvency practitioners, external accountants, and tax advisers;

(f) independent legal professionals, in accordance with the applicable law;

(g) trust or company service providers;

(h) estate agents and real estate developers, but only in respect of transactions for which the monthly rental value is the entire equivalent in LEI of EUR 10,000 or more;

(i) other persons trading in goods, but only in respect of cash transactions whose minimum limit is the entire equivalent in LEI of 10,000 EUR;

(j) providers engaged in exchange services between virtual currencies and fiat currencies;

(k) custodian wallet providers;

(l) persons trading or acting as intermediaries in the trade of works of art, when carried out in art galleries, auction houses or free ports, where the value of the transaction or a series of linked transactions amounts to EUR 10,000 or more, in accordance with the applicable law;

MLR, as a set of legislative rules according to the definition provided hereinabove, sets out the requirements for the reporting entities for the purpose of establishing, implementing, and maintaining appropriate policies and procedures through risk-based reporting, with respect to:

(a) Risk management practices (risk-based approach);

[1] excluding occupational pension schemes

(b) Internal control;

(c) Customer due diligence;

(d) Keeping of records;

(e) Compliance monitoring and management with respect to AML and TF; and

(f) Internal communication of such policies and procedures to prevent activities related to money laundering and terrorist financing.

These policies and procedures identify and analyse:

- Complex or unusually large transactions;
- Unusual transaction patterns that do not have a clear economic, commercial, or legal purpose;
- Any other activity that might be considered related to money laundering or terrorist financing.

Although OFS does not expressly fall within any of the categories of persons defined under MLR as a reporting entities, in order to increase the monitoring of the business relationship and determine whether those transactions or activities are suspicious or not, OFS implements AML internal policies with the purpose of:

(a) preventing the use of anonymous services and transactions for money laundering or terrorist financing;

(b) determining whether a customer is a politically exposed person;

(c) ensuring that employees report any suspicious activity/transaction to the Compliance Officer, and the Compliance Officer will take these internal reports into account in the light of the available information and will determine whether they lead to the identification of, or suspicion regarding money laundering or terrorist financing;

(d) Reporting to the competent authorities any money laundering or terrorist financing identified by OFS personnel or its shareholders.

The principles on which MLR are based is **a Risk-based Approach (RBA)**. The RBA includes a series of measures to be taken in order to determine the most cost-effective management method through which the risk of money laundering and terrorist financing faced by a business can be significantly mitigated. The steps on which RBA is based are detailed in Chapter 9 of the AML Internal Policy.

MLR determine what the relevant entities should do, how foreign currency/payment service companies should prevent their services from being used for money laundering or terrorist financing purposes. The AML Internal Policy focuses mainly on preventing and combating money laundering.

Additional information sources:

(a) The National Office for Prevention and Control of Money Laundering: http://www.onpcsb.ro/

(b) The Office of Foreign Assets Control (OFAC): www.treasury.gov/ofac

(c) The Basel Committee https://www.bis.org

(d) OECD http://www.oecd.org/

(e) Transparency International https://www.transparency.org/

(f) FinCEN Advisory list: www.fincen.gov

(g) EU External Action - Consolidated list of sanctions (https://webgate.ec.europa.eu/ https://eeas.europa.eu/headquarters/headquarters-homepage/8442/consolidated-list-sanctions_en

5. INTERNATIONAL LIMITATIONS COMPLIANCE

In view of the international commitments made by Romania as a member state of the United Nations and of the European Union, and in view of the binding nature of the legal provisions relating to international limitations, OFS undertakes to comply with all applicable standards and legal rules on the enforcement, at a national level, of the international limitations established by:

(a) The United Nations Security Council resolutions or other acts adopted pursuant to art. 41 of the Charter of the United Nations,

as well as by means of

(b) Regulations, decisions, common positions, joint actions, and other European Union legal instruments.

The international limitations concern, in particular, the blocking of funds and economic resources, trade restrictions on operations in dual-use goods and technology, etc.

These rules are binding under the national law for all public authorities and institutions in Romania, as well as for natural or legal persons who are either Romanian or located in Romania. National legislation cannot be invoked to justify the lack of enforcement of such international sanctions.

In order to provide the general framework for cooperation in relation to the implementation of international limitations in Romania, the Inter-institutional Council is hereby established. It consists of representatives of the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Internal Affairs, the Ministry of National Defence, the National Agency for Fiscal Administration, the Ministry of Business Environment, Trade and Entrepreneurship - the Foreign Trade Department, the Ministry of Transport, the Romanian Intelligence Service, the Foreign Intelligence Service, the National Bank of Romania, The Financial Supervisory Authority, the National Office for Prevention and Control of Money Laundering.

The Inter-institutional Council will have, inter alia, the following tasks pursuant to art. 14 of GEO 202/2008

(a) providing the consultation framework to harmonize the activities of the Romanian public authorities and institutions related to the implementation of international sanctions;

(b) drawing up and issuing, upon the notified competent authority’s request, advisory opinions for the rationale of international sanctions application;

(c) providing information on the measures taken by Romania for international sanctions implementation purposes, whenever necessary, but at least once a year;

(d) Ensuring, whenever possible, that natural and legal persons who own or control assets are informed of the imminent adoption of international sanctions, so as to enable the implementation of such sanctions upon their adoption and without undue delay.

The implementation modality, categories, the competent authorities, and their functions as well as the non-compliance penalties are provided by law, with direct reference to the provisions of GEO 202/2008 on the implementation of international sanctions.

6. COMPLIANCE WITH OFAC REQUIREMENTS

In addition to the laws and regulations mentioned hereinabove, OFS also complies with the OFAC compliance requirements. It is imperative that OFS management understands and complies with the OFAC compliance requirements. OFS undertakes to filter all transfers from clients by matching them against the lists of names and sanctions provided by the governments of those states and territories in which it operates.

If a potential match is identified, OFS investigates the transfer to determine if the appropriate name refers to the person in the related sanctions list, comparing the name appearing in the chain of transfers with the name in the SDN list and performing an EDD, thereafter reporting the suspicious transaction to NOPCML, as provided by the applicable law.

The Compliance Officer is responsible for conforming to the compliance requirements and provides regular training programs for the relevant personnel in all areas in which our company operates.

In accordance with the regulatory and compliance requirements, OFS ensures ***that all the transfers are monitored and blocked*** in case a suspicion arises regarding, or if OFS has knowledge of, the fact that the following conditions may apply:

(a) the transfers executed in FIAT Currency or Virtual Currencies by or from natural or legal persons listed on the OFAC list of specially designated nationals and blocked persons ('**SDN list'**), or to or from natural or legal persons associated with the SDN list; or

(b) the transactions are made to or from U.S.A (whether by U.S.A citizens or not) or from countries, natural or legal persons on the SDN list; or

(c) the source of funds results from U.S.A or from countries, natural or legal persons on the SDN list

In some cases, a client or a transfer of Virtual Assets from a client may be prohibited, even if there is no blocking interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the property). In these cases, the deposit is simply rejected (i.e., will not be executed).

OFS maintains ***a complete and accurate record*** of each rejected client for at least five years from the date of the client request. In the case of blocked transfers, records must be kept for the duration for which the property is blocked, and for an additional five years after the property is unblocked.

7. GDPR COMPLIANCE

Under Law 129/2019, OFS processes the client's personal data for the purposes of preventing money laundering and terrorist financing, subject to the provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC („**General Data Protection Regulation**" or „**GDPR**").

The General Data Protection Regulation is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). In force since 25/05/2018, the GDPR sets out the following principles to be applied when processing personal data:

Within the scope of its activity, OFS processes personal data in accordance with the principles of the GDPR:

- Lawfulness, fairness, and transparency: Personal data are processed lawfully and in a transparent manner, ensuring fairness with regard to natural persons whose personal data are processed;
- **Purpose limitations**: There are specific purposes for the processing of data and OFS must inform individuals about such purposes when collecting their personal data. OFS cannot simply collect personal data for undefined purposes;
- **Data minimization**: OFS collects and processes only those personal data that are necessary for the purpose for which they were collected;
- **Accuracy**: OFS ensures that personal data are accurate and up to date considering the purposes for which they are processed, and otherwise are rectified; OFS will not use personal data for purposes that are incompatible with the original purpose;

Storage limitations: OFS ensures that personal data are not kept any longer than what is necessary for the purposes for which they were collected;

- **Integrity and Privacy**: OFS has implemented appropriate technical and organizational safeguards to ensure the security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, by taking appropriate technological measures.

For the purposes of the GDPR Regulation:

Personal data means any information related to an identified or identifiable natural person ("the data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

The Data Protection Officer (**DPO**) is the leading figure of the company's security as required by the GDPR. In the exercise of their duty, the DPO takes due account of the risk associated with the processing operations, considering the nature, scope, context and purposes of that processing.

The controller and the processor ensures that the data protection officer does not receive any instructions regarding the exercise of those tasks. He/she shall not be dismissed or penalized by the controller or the processor for the performance of his or her duties. The Data Protection Officer shall be directly responsible in front of the highest management level of the controller or processor.

Under AML laws, OFS stores personal data for 5 years after the termination of the customer relationship, unless other legal provisions require that data to be retained for a longer time period.

To ensure compliance continuity with respect to the applicable laws on personal data protection, a data Protection Officer (DPO) has been appointed in OFS and can be contacted in writing by email to compliance@chainways.eu.

Likewise, OFS protects the security and privacy of all customers by implementing appropriate technical and organizational measures to ensure compliance with the GDPR provisions.

OFS regularly provides appropriate training to employees on the relevant personal data protection requirements.

OFS's compliance with the GDPR requirements is supplemented by the company's implementation of GDPR related documents. The data subject's rights are more thoroughly explained by the instructions set forth in OFS's Annex on the personal data protection policy.

8. THE COMPLIANCE OFFICER ("AML OFFICER" OR "MLRO")

For enhanced transparency and security, OFS appoints one person as responsible for the implementation of the AML internal policy and, more broadly, with all the MLRO related regulations, as well as with the obligation to determine the nature and extent of the responsibilities entrusted.

The Compliance Officer *(MLRO)* is the person within an organization who is responsible for overseeing all activities related to anti-money laundering issues.

Given the nature of the responsibilities entrusted to the MLRO, OFS puts in place protection mechanisms for the MLRO and its potential assistants, including granting the right to address in its own name, to report any kind of money laundering and terrorist financing law violations within the entity, to the state authorities, in which case the identity of such persons will be adequately protected.

The mechanics for the protection of the MLRO and responsible persons include, where appropriate, at least the criteria laid down in art. 23 para. (6) of Law 129/2019, including:

- specific procedures for receiving reports regarding any kind of law breaches and for taking subsequent measures;
- the protection of the personal data of the person who reports a breach of any kind of the MLRO, as well as of the natural person suspected of being responsible for the breach, in accordance with the principles laid down by GDPR;
- Clear rules ensuring that confidentiality is guaranteed in all cases with regard to the identity of the person reporting the breaches committed within the entity, unless disclosure is required by other legal provisions.

9. TRAINING OF PERSONNEL AND REPORTING

OFS will consider, during its recruitment processes, the knowledge and skills of each individual recruited in relation to the knowledge and skills required for the specific position for which the person is applying. However, regardless of a position's assessed risk, all employees will complete, on an annual basis, an AML training course, as well as a training for identifying and reporting unusual activities or transactions that may prove suspicious.

Moreover, the personnel dealing with operations which may have a higher risk level, will undergo special training: such training will include a better understanding of the policies and processes, of the monitoring processes for suspicious activity, the means of reporting suspicious activity, latest regulatory changes, newly appeared risks in respect of TF and ML as well as a presentation of various typologies thereof.

The AML training program has been designed to ensure that employees understand:

- the AML legislation;
- the risks of money laundering/terrorist financing for the company and the minimum concepts regarding the assessment thereof;
- the consequences of non-compliance with AML procedures;
- the identity and responsibilities of the AML agent;
- the KYC procedures;
- the company's internal systems and controls;
- what to pay attention to regarding suspicious transactions;
- how to submit a suspicious activity internal report;
- the record keeping requirements;
- any information on the training and feedback provided by NOPCML;
- Relevant practical issues arising from its own activity and, where appropriate, from its group, including typologies and case studies.

OFS periodically verifies all persons holding duties related to the enforcement of the measures set forth in KYC policies in order to ensure that they are adequately prepared for the performance of such duties. The verification process includes, in particular, those departments which are found not to report suspicious transactions carried out through them and subsequently identified by the company, if the elements of suspicion were detectable at their level, as well as those departments for which internal checks have shown deficiencies.

OFS may apply different mechanisms to ensure that the AML training program objectives are fully achieved and understood, including:

- on-line corporate training;
- training programs presented by the trainer;
- personalized training programs accordingly paced for each participant;
- Compulsory reading of training materials. All OFS personnel (including new employees) are required to undertake AML training within 3 months of starting their employment with OFS and thereafter undertake annual training in line with this policy.

OFS's or its staff's compliance with reporting obligations does not constitute a breach of a disclosure restriction imposed by a contract or by an act holding legal authority, regulation or administrative act, and does not entail any liability for the entity or its employees, even if they have not known precisely the type of criminal activity, or any kind of violation of the law, regardless of whether that activity took place or not.

OFS acknowledges and undertakes its obligation to provide legal protection for those employees and representatives who report, either internally or to NOPCML, money laundering or terrorist financing suspicious activity, exposure to threats, retaliation, or hostile acts, in particular to unfavourable or discriminatory acts in the workplace, including the confidentiality of their identity.

10. EXISTING / EMERGING RISKS IN MONEY LAUNDERING AND TERRORIST FINANCING (ML / TF)

In addressing the assessment and management of money laundering/terrorist financing risks related to occasional business relationships and transactions, OFS includes the following:

- activity-wide risk assessments;
- customer due diligence;
- achieving an overall vision;
- Monitoring and review.

The risk assessment must therefore consist of two separate steps:

(a) The identification of the money laundering/terrorist financing risk; and

(b) The assessment of money laundering/terrorist financing risk.

10.1 RISK IDENTIFICATION

The identification of ML/TF risks is mainly based on the diversification of information sources and on risk factors structuring. In line with the recommendations in place at European level, OFS will take into account, in terms of information sources, at least the following:

- risk assessment by the European Commission at supranational level;
- information from the government, such as national risk assessments carried out by the government, political statements, and warnings, as well as explanatory statements for the relevant legislation;
- information from regulatory authorities, such as guidelines and reasoning for infringements fines;
- Information from financial intelligence units and law enforcement agencies, such as threat reports, alerts, and typologies; and information obtained in the course of the application of standard CDD measures.

In terms of risk factors, OFS internal AML policy keeps a non-exhaustive list of the risks associated with its activity, also based on an overview of all the elements that need to be corroborated in order to fit a particular relationship in a particular risk category. OFS is highly cautious in relation to its customers and partners due to exposure to the following risks:

10.1.1 The country risk is the assessment of a country's or jurisdiction's vulnerability to ML, TF and of the targeted financial sanctions.

Risk factors:

- targeted financial sanctions;
- AML concerns;
- terrorism concerns/lack of counter-terrorism verifications;
- concerns about illicit drug trafficking;
- corruption related issued;
- money laundering concerns;

Low geographical risks

Clients located in or having the funds in:

- Member States;
- third countries with effective anti-money laundering and anti-terrorist financing systems;
- third countries identified from credible sources as having a low level of corruption or other criminal activity;
- third countries which, on the basis of credible sources such as mutual evaluations, detailed evaluation reports or published monitoring reports, have laid down anti-money laundering and anti-terrorist financing requirements in accordance with the recommendations of the revised Financial Action Task Force and they effectively implement those requirements.

High geographical risks

Clients located in or having the funds in:

- countries which, according to the assessment of international bodies, do not have effective anti-money laundering / anti-terrorist financing systems;
- countries which, according to credible sources, have a high level of corruption or other criminal activities;
- countries subject to sanctions, embargoes or similar measures, established, for example, by the European Union or the United Nations;
- countries that provide financing or support for terrorist activities or on the territory of which designated terrorist organizations operate.
- countries on the OFAC List

10.1.2 **Client risk** – is identified based on the risk profile of that customer.

Customers with lower risk of ML/TF:

- Customers who are employed/ hold a position or have a regular source of income from a known source that can support the activity carried out; (this also applies to pensioners or social assistance beneficiaries, or to those whose income comes from their life-partners' employment);
- Customers with an active and long-term business relationship with the company; and
- Customers representing those whose appointment is subject to court approval or confirmation (such as bailiffs);
- public companies listed on a stock exchange and subject to the disclosure requirements, either by stock exchange rules or by law or by means of enforcement, which impose requirements to ensure adequate transparency of the beneficial owner;
- public enterprises;
- Customers residing in low-risk geographical areas.

Customers with high risk of ML/TF

- if the business relationship takes place in unusual circumstances;

- if clients are residing in high-risk geographical areas;
- if the client is a legal entity or entity without legal personality acting as structures for the management of personal holdings;
- companies with nominee shareholders or bearer shares;
- the client is active in activities with a lot of cash turnover;
- clients with unusual or excessively complex shareholding structure, considering the nature of its activity;
- clients on the OFAC List

10.1.3 **Channel (delivery) risk** – is determined by assessing whether the delivery of the service involves face-to-face contact with the customer, because face-to-face contact limits client anonymity and makes it easy to determine whether they are those who they claim to be. Using third parties as part of a product or service delivery chain also entails a higher channel risk for ML/TF.

10.1.4 **Risk of non-direct (face-to-face) interaction** – assesses the extent to which customers do not interact face-to-face. If a customer does not interact in person (face-to-face), there is an increased risk that they may not be who they claim to be, which can contribute to classifying the channels used by the company as presenting a higher risk for ML/TF.

10.1.5 **Operational risk** – losses due to inadequate or failed internal procedures and systems, human errors, inadequate data processing, external events, etc.

10.1.6 **Concentration** risk — losses due to exposure to a particular asset category or counterparts. A lack of knowledge about a particular customer or about who is behind that customer, or what the customer's relationship with other debtors is, may put the institution at risk from this point of view.

10.1.7 **Reputational risk** – is the potential damage of adverse publicity regarding business practices and business associations that, regardless of its accuracy, will cause a loss of public confidence in the integrity of the entity.

10.1.8 **The legal risk** is the complete failure to comply with the applicable regulatory framework, which may involve regulatory fines or even criminal prosecution. This risk may also involve potential judicial procedures, adverse rulings, unenforceable contracts, increased costs, etc.

10.1.9 Emerging ML/TF risks:

(a) **Virtual currencies related risks:** Due to the fact that historically most of the wallets were not identified and within trading platforms there is a limited trackability on the transfers of virtual currencies, when clients deposit virtual currencies for trading and based on our internal verification we observe unusual transfer patterns in the blockchain for the wallets which were passed by the analysed virtual currencies, such event will be flagged as a high risk.

(b) Cyber attacks

- Any type of offensive handling method involving information systems, infrastructures, computer networks or personal electronic devices. May be employed by countries, individuals, groups, societies, or organizations;
- May originate from an anonymous source.
- Data protection;

10.2 RISK ASSESSMENT

Risk assessment is the second step of effective risk management and is based on the principle of risk-based approach.

Risk-based approach means to assess the risks in order to prevent and combat money laundering and terrorist financing and to implement appropriate management and mitigation measures of these risks. The actual ML/TF risks that our business faces and the implementation of measures for the management thereof. A risk-based approach must balance the costs borne by the business or customer with a realistic risk assessment that our company might be exploited for ML/TF purposes. This allows us to knowingly focus our efforts on the highest risk areas, and to reduce the unnecessary burden on low ML / TF risk customers.

OFS complies with the obligation to apply a policy for carrying out and updating risk assessment, considering risk factors, including those relating to customers, countries or geographical areas, products, services, transactions, or distribution channels in accordance with the provisions of art. 25 of Law 129/2019.

OFS updates the risk assessments and the policy for carrying out and updating the risk assessments as necessary **on an annual basis**, including taking into account changes in the OFS's development strategy and organizational structure.

Prohibited Business/commercial relations

OFS will refuse to complete a business relationship or will not enter a business relationship and/or reject any operations related to the following scenarios:

OFS cannot reasonably identify the true identity of the customer and/or of the UBO, or if the formal requirements relating to customer identification and/or UBO are not met. OFS is required to obtain evidence of the registration of beneficial owners, or information from the beneficial owner's central registers, whenever it enters a new business relationship with a person who is subject to UBO information registration requirements,

- If the nature of the customer’s business is unclear;
- If they suspect that the customer has engaged, engages, or may engage in illegal activities/transactions;
- If the customer’s assets are known to represent or suspected of being the result/proceeds of criminal activity;
- If it suspects that the customer is involved in corruption, bribery and/or tax evasion;
- If the customer is known to be, or suspected to be, a terrorist, a drug and/or humans’ trafficker, a criminal organization, a member of it, if the customer is listed on the sanctions list or they come from a sanctioned listed country;
- If it suspects that the customer maintains anonymous, shell, or transitional accounts.

The risk assessment methodology

The risk assessment is the way of identifying the risks our business is exposed to. We must be able to understand all the ways that our business could be exposed to money laundering and terrorism financing risks, and design systems to prevent and deal with them.

Actions:

(a) identifying and monitoring the risks of money laundering and terrorist financing that are relevant to our business in other words, our business's risk assessment;

(b) taking note of information on risk and emerging trends from risk assessment sources;

(c) assessing, and keeping under regular review the risks, including those posed by the following:

- customers and any underlying beneficial owners;
- the source of funds;

The risk assessment is in writing and is kept up to date. It reflects the changes in the business and the environment in which we operate. At least an annual review of the risk assessment is recommended, and any revisions noted in the document.

***"*Suspicion**" can occur in circumstances that suggest to a reasonable individual that a person might be laundering money. Suspicion must be more than a mere hunch; it must be evidence based and it must be settled (i.e., the reasonable individual must have considered all readily available evidence). Any activity that does not fit with the normal course of the company or is not normal for a particular client should be regarded as suspicious.

Suspicious indicators: *New customers*

- Checking identity is proving difficult.
- The client is reluctant to provide details of their identity.
- The client will not disclose the source of funds.
- The explanation for the business and/or the amounts involved are not credible.
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks.
- The client has made an unusual request for collection or delivery.
- Transactions having no apparent purpose, or which make no obvious financial sense, or which seem to involve unnecessary complexity.

Regular and established customers

- the transaction is different from the normal business of the client;
- The size or frequency of the transaction is not consistent with the normal activities of the client.
- The pattern of transactions has changed since the business relationship was established.

Examples where customer identification issues may point to suspicious activity (the Joint Guide under Article 25 of the (EU) Regulation 2015/847)

- The client refuses or appears reluctant to provide information requested.
- There appears to be inconsistencies in the information provided by the client.
- The client's area of residence is inconsistent with other profile details such as employment.
- An address appears vague or unusual.

- The supporting documentation does not add validity to the other information provided by the client.
- The client is in a hurry to rush his activity through, with promises to provide the information later;
- There are media articles regarding potential suspicious activity of the potential client.

Examples of activities that might suggest to staff that there could be potential terrorist activity

- the client is unable to satisfactorily explain the source of income or capital.
- frequent address changes.
- media reports on suspected or arrested terrorists.

11. CUSTOMER IDENTIFICATION AND DUE DILIGENCE

OFS has established a Know Your Client (KYC) procedure to ensure that the identities of all new and existing clients are verified to a reasonable level of certainty. OFS applies KYC measures to all new and existing customers, depending on the risk, or when the relevant client circumstances change or if the reporting entities have a legal obligation to contact the customer in the relevant calendar year to examine all relevant information relating to the ultimate beneficial owner.

This will include all individual clients, all directors and shareholders with a stake holding of **25% or more** in the client companies. The identities will be verified on-line using KYC and AML reputable service providers. In addition, OFS will comply with all the KYC requirements laid down by the MLR, in particular by Law 129/2019, and will take steps to keep the KYC policy constantly updated in accordance with applicable law.

Who is the customer*?*

The customer is the person or entity with whom OFS enters into virtual asset management services.

OFS will collect customer information and implement KYC measures from which it can establish:

- who the customer is (as well as verifying their identity);
- who owns the customer (including ultimate beneficial owners);
- who controls it;
- the nature of the customer;
- the source of the client's investment funds and whether the client's financial situation allows the client to invest;
- the source of the client’s virtual assets

When establishing a business relationship, in order to determine the risk profile of the individual client, OFS obtains information on at least the following:

(a) surname and first name, if any;

(b) date and place of birth;

(c) the personal identification number or, where applicable, a similar unique identifier;

(d) the series and number of the ID document used,

(e) the address at which they reside, and the identification of their tax and legal regime, i.e., if it is a domicile, residence, or other similar identifier;

(f) nationality;

(g) the occupation, position and, where applicable, the name of the employer or the nature of their own work;

(h) telephone number, fax, e-mail address, if any;

(i) investment experience;

(j) personal property;

(k) the source of funds/virtual assets to be used in the context of the business relationship;

(l) the classification as publicly exposed persons or as a family member of a publicly exposed person, or a person known to be a close associate of a publicly exposed person;

(m) the ultimate beneficial owner information, if different from the customer;

(n) information if the client acts on its own behalf or as a proxy.

When establishing a business relationship, in order to determine the risk profile of the corporate client, OFS obtains information on at least the following:

(a) the name and identification data of the company;

(b) the registered office;

(c) the scope of activity;

(d) legal representative(s) and their identification data;

(e) telephone, e-mail, web page;

(f) trade registry excerpt or equivalent;

(g) proxy documentation, if the representative is not its director;

(h) shareholders, their identification data, and ownership percentages;

(i) sole registration code or equivalent

(j) data relating to the ultimate beneficial owner;

(k) account manager data;

(l) tax details of the company;

(m) the source of funds/virtual assets to be used in the context of the business relationship;

(n) investment experience;

(o) information if the client acts on its own behalf or as a proxy.

For the purpose of the provisions hereinabove, in accordance with **art. 15 of Law 129/2019,** the identification of customers and ultimate beneficial owners comprises, at least:

- in the case of natural persons - all civil status data provided for in the ID documents set forth by the applicable law;
- in the case of legal persons - the data included in the articles of association or registration certificate, and the data of the legal representative of the legal person entering into the contract;
- the data and information provided for in the applicable sector-specific regulations.
- in the case of foreign legal persons, a certified translation into Romanian of the articles of association /registration certificate will be requested, respectively the data of the legal representative of the legal person that concludes the contract with the payment institution.

CDD/KYC Customer due diligence (CDD) – or know your Customer (KYC) means:

- identifying all customers and verifying their identity;
- identification and verification of the identity of the ultimate beneficial owner, including in relation to legal persons, trusts, companies, associations, foundations and similar unincorporated entities, and understanding of the ownership and control structure of the client;
- obtaining information about the intended purpose and nature of the business relationship;
- conducting ongoing monitoring of the business relationship to ensure that the funds used for the acquisition of the virtual assets placed under OFS's management are consistent with what is known about the customer and for risk assessment purposes;
- record keeping of such checks and updating thereof accordingly.

OFS ensures that KYC measures are applied to all existing customers prior to entering into any new contractual relationship or to older clients as soon as possible, depending on the risk, but no later than 18 months after the approval of the policies by the management bodies.

In the event that OFS is unable to apply the said provisions, the provisions of art. 11 (9) of Law 129/2019 become applicable. In particular, it will not initiate or continue the business relationship and will draw up a suspicious transaction report in relation to the customer concerned whenever there are grounds for suspicion, which will be transmitted to NOPCML **under art. 11 (9) from Law 129/2019.**

Due Diligence is performed not only for all new customers but also for existing customers, at appropriate time intervals on a risk-sensitive basis, when the client's relevant change occurs or when the entity has a legal obligation in this regard. All transactions / clients require a degree of risk assessment to determine that they are on the lower risk spectrum and require continuous monitoring.

11.1 The Due Diligence Procedure

Simplified Due Diligence is applied in relation to a particular business relationship, if after a full risk assessment was carried out it is determined that the business relationship represents a low degree of risk of money laundering and terrorist financing.

In order to apply simplified due diligence, OFS will ensure that:

- It is supported by the customer's internal risk assessment;

- The customer is identified, and its identity can be verified;
- The identity of the beneficial owner is known, and its identity can be verified, as well as its ownership percentage:

In which case:

- EDD does not apply;
- we monitor the business relationship to ensure that nothing unusual or suspicious exists from the start;
- is not hindered by information on risk provided by any other authority in periodically published risk assessments;
- the customer is not a politically exposed person, a family member or a known close associate of a politically exposed person (*as per* art. 11 para. 3 of Law 129/2019).
- the source of funds or virtual assets is transparent and understood by our company;

The assignment to a low risk level is achieved through an overall assessment of all identified risk factors. In accordance with the provisions of art.11 (6) of Law 129/2019, when assessing the money laundering and terrorist financing risk, OFS is obliged to take into account at least the following:

(a) the purpose of initiating a business relationship with the company;

(b) the investment and withdrawal amount that the customer intends to make through OFS;

(c) the duration of the business relationship;

(d) Sector-specific regulations and instructions issued by the authorities referred to in Article 1(4) of Law 129/2019 or the relevant regulatory authorities

The low-risk classification is carried out in accordance with the provisions of Article 16 (2) of Law 129/2019 taking into account at least the following characteristic factors:

(a) customer risk factors;

(b) risk factors relating to products, services, transactions or distribution channels;

(c) geographical risk factors;

Special procedures apply for PEP, in particular in certain countries, and for accounts opened by or through foreign banks.

This may require us to review the degree of diligence undertaken, for example, by applying enhanced due diligence if the customer presents a higher risk, meaning, in particular, taking general precautions such as:

- not having business relations with certain persons or entities if we cannot ensure proper customer due diligence and if we believe that a suspicious business report is necessary;
- having a system for keeping copies of CDD and documentary evidence and keeping such information up to date;
- suspecting money laundering or terrorist financing;
- doubting whether the documents obtained for identification are authentic;

- doubting whether the person is indeed the one shown in the documentation;
- suspecting that documents obtained for identification could be lost, stolen or unlawfully acquired;
- circumstances have changed and the risk assessment no longer considers the client, its transactions or its location to be low risk.

If we are unable to complete CDD measures, the customer's account will not be opened, and no commercial activity will be initiated.

Enhanced due diligence/EDD measures are necessary in high-risk cases (e.g., relations with PEPs), high risk sectors, as mentioned above, countries officially designated as being high risk with a high level of money laundering, terrorist financing and corruption, shell companies, companies with nominated directors or stakeholders, etc.

Whenever a client has been identified as posing a higher risk of money laundering, it should be redirected to the EDD compliance officer so that a wider verification or monitoring can be carried out.

Under Law 129/2019, enhanced EDD and continuous monitoring measures will be applied in order to manage and mitigate risks arising in all situations which, by their nature, may pose an increased risk of money laundering or terrorist financing, including in the following situations:

- in any case identified as one where there is a high risk of money laundering or terrorist financing;
- in any business relationship with a person established in a high risk third country;
- in the case of business relations with publicly exposed persons or with customers whose ultimate beneficial owners are publicly exposed persons, including for a period of at least 12 months from the date on which that person no longer occupies a significant public position;
- complex transactions;
- transactions with unusually high values, i.e., above USD 250.000;
- do not fit the usual pattern;
- have no obvious economic, commercial, or legal purpose.
- in any other case which, by nature, may pose a higher risk of money laundering or terrorist financing. In addition, based on FATF recommendations, we apply EDD measures if the following cases are identified:
- multi-jurisdictional and/or complex structure of entities and/or trusts;
- external payments without a clear link to the actual activities of the corporate entity;
- the use of offshore bank accounts without a clear economic need;
- use of nominated directors;
- use of shell companies.

As with our standard CDD, EDD also consists in the monitoring of the performed activities. In addition to the more complex verification process, improved continuous monitoring measures are applied throughout the business relationship.

In relation to transactions involving persons from countries with vulnerabilities in terms of money laundering and counter-terrorist financing prevention systems, and which do not apply or apply international standards insufficiently, OFS will examine the circumstances and purpose of such transactions, considering that the EDD measures must include (according to art. 17 (6) of Law 129/2019):

(a) obtaining additional information about the customer and its ultimate beneficial owner;

(b) obtaining further information on the expected nature of the business relationship;

(c) obtaining information about the source of funds and the source of wealth of the client and the beneficial owner of the client;

(d) obtaining information on the reasons for the transactions;

(e) obtaining senior management approval to establish or continue the business relationship;

Other EDD measures may include:

- financial statements and bank references;
- a detailed structure of the company's chain of ownership;
- the legal domicile/real business address of the legal person;
- description of the business operations, expected volume of currency and total sales, etc.;
- an explanation of any change in the corporate structure or account activity;
- additional screening / negative news research;

Remote identification and verification (not face-to-face)

This entails an inherent risk of impersonation fraud.

In some extreme cases, there may be scenarios where the identity of the customers is verified electronically, the company will apply an additional verification to manage the risk of impersonation fraud. The additional checks that the company can perform consist of thorough fraud checks, carried out routinely, as part of the existing policies or as part of other measures, such as:

- the verification of additional aspects of the customer’s identity;
- telephone contact with the customer prior to opening the account on a residential or business number that has been verified (electronically or otherwise) or a "welcome call" to the customer before allowing operations, using it to verify additional aspects related to their personal identity, information that was previously provided during the creation of the account;
- communication with the customer at a previously mentioned address;

However, the effective start of the management of digital assets will not take place until the client is met in person, by a OFS employee or partner.

The entities, when applying KYC measures, are required to keep them in electronic or paper readable form in other form acceptable in the context of legal proceedings, all records obtained through the application of these measures, such as ID copies, performed monitoring and verification documentation copies, including the information obtained by

electronic identification means necessary to meet KYC requirements, for a period of 5 years from the date of termination of the business relationship with the customer.

Adverse media screening ***The Risk Factors Guidelines under the EU's 5th AML directive outline the need for legal entities to perform adverse media searches as part of EDD process for high-risk customers.*** In addition, FATF Recommendations states the following: "Financial institutions should understand the client's reputation, including if they were previously investigated for money laundering, terrorist financing or if they faced regulatory penalties. *In essence, an adverse media check is necessary when dealing with high-risk customers."*

Regardless of its client's risk rating, OFS performs adverse media screening on all its clients as part of the customer due diligence process and ongoing risk assessment, ensuring that OFS meets its regulatory requirements and obligations. The purpose of a proper verification of adverse media articles from different sources is to expose the involvement of an individual or an organization in money laundering, terrorist financing, financial fraud, missile, organized crime and other criminal activities.

Adverse media sources include:

- Traditional news and media sources;
- Databases of international organizations;
- Blogs and web articles - including websites publishing corruption-related issues, missile-related activities and financial fraud;
- Social media and internet. Adverse media is sufficient reason to perform an EDD on a customer or their beneficial owner. The scope of adverse media is not limited to an allegation or conviction related to financial crimes; a client's bad reputation is enough to pose risks.

Gender reassignment

In case of gender reassignment, the company will make sure (for instance, based on documentary medical evidence and face to face interview) that the gender transfer of a customer is genuine (similarly to name change cases). Such cases usually involve the transfer of a credit history to a reassigned gender. This may involve data protection, not money laundering issues. The consent of the person involved may be necessary. However, an electronic verification report with the alias added would normally verify the client successfully.

Source of funds verification Acceptable evidence includes:

- bank statements not older than 1 month;
- a letter of secured or unsecured loan;
- the employee's payslip or employment agreement;
- annual income (confirmed for example by annual tax return);
- collection of documentary evidence on the source of funds;
- sale deeds;
- GMS resolutions for the payment of dividends;
- Loan/trust agreements;

- A savings bond, an inheritance certificate;
- A donation or manual gift agreement;
- proof of acquisition/mining of the transferred virtual assets (for each virtual asset separately);
- another appropriate document.

After EDD is completed, there ***are two options***:

(a) we may end the relationship based on a supporting notice, and not enter into a virtual asset management agreement or terminate the existing agreement (this option is normally taken when the risk outweighs the benefit of having a relationship with this client);

(b) we accept the high-risk relationship, but we implement a detailed monitoring plan and risk mitigation activities that can alleviate our exposure to risk.

12. CORPORATE SERVICES - THE CLIENTS' VIRTUAL ASSETS MANAGEMENT PROCEDURE

Individuals' identification

***General requirements* for KYC documents:**

- Must have all details clearly visible/legible;
- Must have all four corners showing;
- Must be valid and unaltered by computer software;
- The copy must be clear, with all details clearly visible/legible, showing all four corners;
- If visibly damaged (cut, torn up and glued, washed-out information, etc.), cannot be accepted;
- If handwritten - cannot be accepted;
- If expired (or set to expire within the next 24 hours) - cannot be accepted.

Proof of Identity- What is normally checked?

- Photo must be clearly visible and similar to other ID photos of the potential customer, if the potential customer has other photographs on the file;
- The date of birth must match the profile;
- The date of issue and expiry. The expiry period must correspond to the type of documents (e.g., ordinary passports issued in Romania expire 10 years after issuance);
- Security printing: watermarks, holograms, geometric lathe work, etc;
- When ID issued by the relevant authority expires, the client must provide a valid ID - no restrictions.

At least one of the following documents are provided in good, clear, and coloured copy. If necessary, the document has to be officially certified/notarised.

- Current signed passport;

- EEA national ID card;
- National ID card (non-EEA);
- Current travel document;
- Immigration application card;
- Driving license;
- Residence permit.

If the prospective client provides a false or to us a fake or doctored ID, they will be blocked from ever having an account on OFS's platforms. OFS may also, if necessary, notify the authorities of any such attempt to use these documents.

OFS will consider an acceptable proof of address:

- utility service invoice (telephone, gas, electricity bills),
- identity card;
- residence permit;
- an excerpt from the national population database;
- Bank statement showing transactions. Proof of address must not be less than 90 days old, except for French residents. Customers from France must provide proof of address not exceeding 75 days from their date of issue as per internal regulations.

Red flags:

- If the potential customer comes from a high-risk country;
- If the potential customer is a PEP or is related to such a person;
- If the potential customer provides a phone number from another country;
- If the address provided is marked as 'non-existent' by Google Maps;
- If the potential customer is uploading documents for another person;
- Whether the potential customer informs the support service that it does not recognize that they did not intend to entrust, or have entrusted the virtual assets for management and trading purposes;
- If the potential customer comes from a country with poor documentation or has low quality and low security for documents (e.g., India).

The ultimate beneficial owners: OFS will ensure that it fully understands the client's legal form, structure, and ownership, and must obtain sufficient additional information on the nature of the client's business, and the reasons for seeking the company's product or service. 'Beneficial owner' means any natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction, operation or activity is carried out. The legislation in force defines the term "beneficial owner" by reference to the various entities involved, as follows:

According to art. 4 of Law 129/2019, "**beneficial owner**" means:

(a) the natural person or persons who ultimately own or control a legal person by exercising the right of ownership, directly or indirectly, on a number of shares or voting rights sufficiently large to ensure their control or by participating in their own

capital of the legal person or by exercising control by other means, the legal person owned or controlled being not a legal person registered in the trade register whose shares are traded on a regulated market and which is subject to advertising requirements in accordance with those regulated by European Union law or with internationally standards. This criterion is deemed to be met where at least 25 % of the shares are held plus one share or share in the equity of the legal person in a proportion exceeding 25 %;

(b) the natural person or persons who ensure the management of the legal person, if, after exhausting all possible means and provided there are no grounds for suspicion, no natural person is identified in accordance with point 1 or if there is any doubt that the identified person is the real beneficiary, in which case the reporting entity is obliged to retain and record the measures applied in order to identify the real beneficiary in accordance with point 1 and this point;

General rules:

- Each potential customer must be checked and evaluated individually. Although all rules apply to all customers, new rules can be introduced from time to time and reasonable exceptions to some rules may be made, which are not legally binding provided they are approved / signed off by the compliance officer.
- All data from all potential clients must be recorded in our internal files.
- To avoid the risk of a unique error source, potential customers should be checked by more than one member of the compliance team until they are approved.
- Whereas, in normal circumstances, the documentation set out herein will be sufficient to verify a client for KYB purposes, if such documentation shows problems or risks which are not clearly visible, the compliance team reserves its right to request additional documentation that is reasonably necessary to properly fulfil the legal, regulatory and payment mechanism rules obligations of the company.
- All registration documents that are still under review in the system are reviewed within 48 hours of receipt. Except as mentioned above, documentation that requires more detailed research or special approval shall be given an additional 24 hours for review.
- If companies do not meet KYB requirements due, inter alia, to suspicious documentation, suspicious activity, listing on a blacklist by a government body or regulator, insofar as it includes their company or their website, negative reviews, or manifestly false signatures, the deadlines hereinabove will not apply and a full detailed report will be required and submitted to the compliance verification team for further submission to the committee, for approval or rejection.

KYB verification the documentation / information checked includes the following:

- the Company’s website;
- KYC of all legal representatives, administrators, directors, shareholders, and beneficial owners of the customer;
- the ultimate beneficial owner statement (UBO);
- Articles of association/statutes/other equivalent incorporation document;
- Trade registry certificate, not older than 30 days old;

- the last financial statements of the company;
- Statement of account issued in the name of the company, not more than 30 days old;

NOTES:

- Corporate documentation must be provided according to the standards of the country's registration requirements.
- For every person mentioned in the corporate structure, it is mandatory to ask for the complete KYC information and to ensure that it does not appear on the OFAC list and the PEP list.
- Corporate documents that are not in Romanian shall be formally translated into English and duly certified.
- Most EU countries have no ownership/share confirmation certificate. In such cases, a recent company excerpt and the articles of association are sufficient.
- Regarding the bank statements of the potential customer, a downloaded PDF version of the bank statement must be submitted, including the bank and company's details on the document header. A bank letter shall not be classified as a bank statement and such statement shall not exceed 30 days from the date of the submission of the application. Please note that the term of the bank statement includes the bank statements provided by another regulated payment institution or an authorized electronic money institution.

Details in the KYC & AML form must be fulfilled accordingly and match the KYB Company we have in the file - company name, registration number, incorporation date, address, directors and shareholder details.

The activity of the potential client's business must be clearly detailed in the request.

If the request presents a different primary address compared to the corporate data, the potential customer must provide official proof of the new address.

The bank accounts mentioned in both documents must belong to the applicant business company. If not - permission to use a bank account + KYB is required for the company holding the bank account. Personal bank accounts cannot be used.

The agreement and the application may not be filled-in in pencil. They must be filled-in only in fountain pen/ ballpoint pen or computer typewritten and properly signed with a pen, certified electronic signature or adobe sign.

The profile address of the potential customer must match the corporate address. If it does not match – then it must be changed.

Deadlines for the provision of missing data:

- Important KYB, KYC or any other documentation requested: 2 weeks

If the potential customer has a sophisticated corporate structure and/or nominal positions (directors or shareholders), benefits from trust services, offshore companies or any other form of anonymity assurance, EDD must be performed until full transparency is achieved and the UBO is identified. Additional required documentation:

- Nomination agreement;
- POA (Power of Attorney)

- Trust/custody statement
- SBO (beneficial ownership statement)
- Any additional documentation that may be relevant.

If the above documentation is missing, then the potential customer is required to provide the full KYB of the company.

13. POLITICALLY EXPOSED PERSONS (PEPs)

For the purposes of Law 219/2019 art. 3, publicly exposed persons are natural persons who exercise or have exercised important public functions:

(a) heads of state, heads of government, ministers and deputy ministers or secretaries of state;[2]

(b) Members of Parliament or similar central legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of the supreme courts, of the constitutional courts or of other high-level courts whose decisions can be challenged only by extraordinary legal remedies;

(e) members of the governing bodies of central banks;

(f) ambassadors and senior officers in the armed forces;

(g) members of the boards of directors and supervisory boards and persons holding management positions in state owned companies;

(h) Directors, deputy directors and members of the board of directors or members of the governing bodies of an international organization.

None of the categories set out above do not include persons in intermediate or lower positions.

Family members of the publicly exposed person are, for the purposes of the DSB:

(a) the spouse of the publicly exposed person or his/her concubine / the person with whom he / she is in relations similar to those of the spouses;

(b) children and spouses or their concubines, persons with whom children are in relations similar to those of the spouses;

(c) Parents.

The siblings of the PEP should also be treated as “family members”. Beyond this definition, companies should take a proportionate and risk-based approach in assessing whether a particular individual is a member of the family of a PEP – for instance, it may be appropriate to deal with a wider circle of family members (such as aunt and uncle) subject to enhanced due diligence in cases where a company has assessed a PEP as posing a higher risk.

Persons known to be close associates of persons publicly exposed shall be:

(a) the natural persons known as the real beneficiaries of a legal person, of an entity without legal personality or of a legal arrangement similar to them together with any

[2] The National Integrity Agency shall draw up the list of important public functions provided for in national law, based on data and information immediately submitted by the entities in charge with such obligation. The National Integrity Agency shall update this list based on the data and information communicated by the entities in charge with such obligation, submitted no later than 5 days after the change has occurred.

of the persons mentioned in paragraph (1) or as having any other close business relationship with such a person;

(b) the natural persons who are the only real beneficiaries of a legal person, of an entity without legal personality or of a legal arrangement similar to them, known as being established for the de facto benefit of one of the persons mentioned above.

Without prejudice to the enforcement, based on a risk assessment, of the additional measures of knowing the clientele, after the expiration of a time limit of one year from the date when the person ceased to hold an important public function within the meaning above, that person is no longer considered as being publicly exposed.

The PEPs are classified into different risk levels and these risk levels give priority to investigating higher risk categories:

Given their location, the PEPs are divided into three types:

- Domestic PEP - politically exposed persons of an internal government body;
- Foreign PEP - politically exposed individuals of a foreign country's government body; and international PEPs - politically exposed person of an international organization established by formal political agreement between two or more countries.
- All customers and clients with owners or controllers that have been identified as PEP represent a higher risk of ML/TF.

If a customer is a PEP, family member or a person close to a PEP, then the following EDD measures will be implemented:

- obtain approval from management before establishing a business relationship with that person;
- taking appropriate measures to determine the source of assets and the source of funds that are involved in the proposed business relationship or transaction;
- Performing enhanced continuous monitoring where we have already entered a business relationship.

In the case of business relationships with publicly exposed persons or persons having as beneficial owner publicly exposed persons, OFS in addition to standard KYC measures, also applies the following measures:

- obtain the approval of senior management for establishing or continuing business relations with such persons;
- take appropriate measures to establish the source of the wealth and the source of the funds involved in business relations or transactions with such persons;
- Carry out on a permanent basis an increased monitoring of the respective business relations.
- The measures referred to in paragraphs (9) and (11) - (13) also apply to family members or persons known to be close associates of publicly exposed persons (Art. 17 (9) of Law 129/2019).

The risk posed by a PEP is assessed using the following matrix:

The type of customer risk		**PEP risk**			
		High	**Medium**	**Low**	**Unknown**
Customers that are high risk	**High**	High	High	Medium	High
	Medium	High	Medium	Medium	High
	Low	Medium	Medium	Low	High
	Unknown	High	High	High	High

Criteria:

Rating	**PEP risk rating**
High	Customers present a severe vulnerability to ML / TF risks, that must be addressed through check measures
Medium	Customers have a moderate vulnerability to ML / TF risks, that must be addressed through check measures
Low	Customers have a minor vulnerability to ML / TF risks, that must be addressed through check measures

The methodology defines and applies consistent criteria when assessing the effectiveness of the check as part

Of the PEP ML/TF risk:

Checks evaluation	
Excellent	Highly effective checks, necessary for the purpose of risk mitigation. Therefore, controls seem to work effectively for the purpose of risk mitigation.
Appropriate	Effective checks.
Weak	Ineffective checks, that appear to be not fit for purpose
No Check /not tested	There are no checks, or the effectiveness thereof has not been tested.

The assessment of the PEP, the EDD should include the following additional measures:

- the assessment of the economic development, employment, corruption and money laundering level, in the countries of residence;

- requesting data on family members or close associates, either empowered to use the account or to receive the Virtual Assets from such account;
- Verifying the publicly available information. Once the EDD has been efficiently carried out, a report will be submitted to the MLRO. He is responsible for taking any decision on the case.

OFS maintains a list of PEP clients, which is verified regularly.

OFS will also record that the customer is subject to increased monitoring, including increased attention to the income and assets reported by the customer. At least 12 months after the customer has ceased to be PEP, the company must assess whether the customer continues to pose an increased risk of ML/TF.

14. REPORTING SUSPICIOUS ACTIVITY

OFS's internal reporting policies. OFS keeps internal procedures that ensure that the employees report suspicious activity to the MLRO. While implementing the policies on suspicious activity reporting, OFS shall refer to the applicable law, including Law 129/2019.

It is the responsibility of all personnel:

- To report transactions and/or customers known to be or suspected of suspicious activity;
- To not make false or misleading reports;
- To maintain the confidentiality of the identity of internal reporting persons and of anyone who may be the subject of such report;
- To assist those who deal with a report, including providing information on request;
- To support personnel reporting suspicious activity, if aware of such report;
- To not retaliate against any other staff member suspected of having reported suspicious activity;
- To immediately inform the MLRO about any suspicions that a repression against an internal reporting person is taking place or that they have been threatened in this regard.

A report must be made as soon as a decision is made that there are reasonable grounds to suspect money laundering. The suspect may appear before or after a transaction takes place.

Reasonable grounds for knowledge or suspicion arise where the facts or circumstances, if examined objectively, would lead to an expectation that a reasonable person might know or suspect that someone is/has/will engage(d) in money laundering or terrorist financing acts.

Before deciding to report to NOPCML, MLRO will need assess all relevant business records, which may include:

- the financial circumstances of the client or of a person on whose behalf the client acts;
- the characteristics of the operation.

In addition, the MLRO will:

- take into account the level of identity information held about the customer and any information held by the customer;
- the personal circumstances which may be available;

The designated officer should also consider any additional risks if the customer is located outside Romania, in particular if the customer is located in a high-risk jurisdiction. If the designated officer decides not to report to NOPCML, the reasons for not doing so should be clearly documented or recorded electronically and kept with the internal suspicious report.

All monitoring systems will produce details of the transactions or activities that require additional assessment, although this does not in itself mean that the activity is confirmed as suspicious. The review and assessment of alerts should be carried out by employees with relevant training and skills, although their specific identity will depend on the individual organization. While reviewing and evaluating day-to-day system-generated alerts is usually a delegated responsibility, the MLRO ultimately has a responsibility to ensure that control procedures are in place for all alerts to be evaluated and recorded and for those records to be kept for future review by regulators and auditors.

If a ***CDD failure*** is discovered, we will ensure that:

- no contract or transfer will be made for such a customer; and
- No business relationship will be established with such a customer. Virtual assets deposited in an account may be reimbursed to the account from where they were transferred.

Mandatory actions:

- termination of any existing business relationship with the customer
- consider making a suspicious transaction report
- If a suspicious transaction report is not made, record the reasons why a report is not considered necessary.

15. RECORD KEEPING

Minimal requirements we maintain:

- copies of the evidence obtained to carry out the customer's due diligence obligations and details of customers' transactions, with for five years after the end of the business relationship;
- details of occasional transactions, for five years from the date of the transaction;
- details of the actions taken in respect of internal and external suspicious reports;
- details of the information examined by the nominated officer in the context of an internal report, for which the nominated officer has not drawn up a suspicious activity report;
- copies of the evidence obtained, if we rely on another person to perform the CDD, for five years from the date of conclusion of the third party's relationship with the customer, and the agreement should be concluded in writing;
- a written record of our risk assessment.
- a written record of our policies, checks and procedures;

- a written record of what you have done to keep staff informed about money laundering and terrorist financing legislation and related data protection requirements, as well as staff training.

Actions required under the following points are examined regularly:

- maintenance of appropriate record keeping systems;
- making the records available, when necessary, within the specified calendar;
- We keep records of customer due diligence checks and business transactions:
  (a) for 5 years after the end of the business relationship;
  (b) for 5 years from the date of conclusion of an occasional transaction;
- We also keep corroborative records for 5 years after a business relationship has ended;
- We keep records of closed branches or agencies.

Record keeping format:

- original documents;
- full photocopies of the original documents;
- scanned forms;
- Digital or electronic forms.

All electronic records will be subject to regular and routine back-up with off-site storage.

The records will be reviewed periodically to ensure, for instance, the keeping of a new copy of expired documents, such as driving licenses or passports. This review will only include ongoing business relations. We are not required to maintain the records of the transactions carried out with those customers that have been part of a business relationship for more than 10 years, if such business relationship is ongoing.

The records will be deleted after the abovementioned period, unless we are required to keep them in connection with legal or judicial proceedings or any other relevant law. Such evidence may be used in judicial proceedings in any applicable jurisdiction.