MANUAL FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING OF

TRINITY TECHNOLOGIES EOOD

January 2024

INDEX

1. INTRODUCTION

1.1. Identifying data

Legal Name: **Trinity Technologies EOOD**

Register Number: UIC207095476

Crypto Authorization: BB - 100/03.10.2022

Registered Address: 2v Topli dol St, ap 16, Sofia, Bulgaria, 1680

1.2. Activity data

Activity data from **Trinity Technologies EOOD** are as follows:

Main activity

Trinity Technologies EOOD provides an exchange service (purchase and sale) of virtual currencies through the **Trinity Technologies EOOD** platform. It supports the following cryptocurrencies:

- Bitcoin
- Ethereum
- Dash
- Bitcoin cash
- Litecoin

(All of them hereinafter referred to as cryptocurrencies)

Cryptocurrency SALE service

Trinity Technologies EOOD acts as an interconnection system between traditional banking platforms and cryptocurrencies allowing the conversion of crypto currencies into legal tender.

For the provision of the service, the Client must have cryptocurrencies in an electronic purse or wallet under their control. **Trinity Technologies EOOD** will buy the Client the equivalent in cryptocurrencies to the cash in euros that he wishes to obtain, discounting the different types of applicable costs.

The Web or application will automatically inform you of the amount in cryptocurrencies that must be sent and the destination public address or wallet.

Sale with Transfer

The client must indicate the data of his bank account in which he wants to receive the money in euros and verify the information summary of the operation before giving the shipping order.

Sales operations will have the following time and economic limits for the provision of services:

SALE	LIMITS	TRANSACTION COSTS	DELIVERY TIME
SEPA TRANSFER	**Sale:** Between 50 € & 20,000 € **Day:** 20,000 €	**Permanent:** 0 € **Variable:** 0.5%	24 business hours
SWIFT TRANSFER	**Purchase:** Between 100€ & 20,000 € **Day:** € 20,000	**Permanent:** 30 € **Variable:** 0.5%	72 business hours

Cryptocurrency PURCHASE service

For the purchase of cryptocurrencies with legal tender, the client must enter the amount of cryptocurrencies that he wishes to acquire, his email address and the public address of his portfolio where he wants to receive the cryptocurrencies on the Web or application.

Next, the user will be redirected to the payment process of the selected Cash-In method, where they must make the payment using their personal credentials.

Once the payment process has been completed, and after the legal tender money has arrived at **Trinity Technologies EOOD**, the user will receive a transfer of cryptocurrencies to their wallet.

Purchase with Bank Transfer

The client must send the proof of payment to **Trinity Technologies EOOD.** In all cases the ordering party, reference and amount must match the registered user and the data previously provided. Otherwise, additional information may be required, even leading to its return.

Purchase with Card

Credit and debit cards are accepted.

Purchase operations will have the following time and economic limits:

PURCHASE	LIMITS	TRANSACTION COSTS	RESERVATION TIME	DELIVERY TIME
TRANSFER	**Purchase**: Between 200€ & 20,000€ **Day:** 20,000 €	**Permanent:** 0€ **Variable:** 0%	After the receipt	24 business hours (When your money arrives at our bank)
CREDIT / DEBIT CARD	**Purchase:** Between 30 € and 5,000 € **Day:** 5,000 €	**Permanent:** 0 € **Variable:** 3%	Instantly	25 minutes

Trinity Technologies EOOD does not exercise any type of financial activity and its purpose is limited to the provision of a virtual currency exchange service through the **Trinity Technologies EOOD** platform located at the following web address crypto-trinity.com through this web platform, users can carry out cryptocurrency purchase and sale operations with **Trinity Technologies EOOD** in accordance with the Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018.

The activity of **Trinity Technologies EOOD** currently, it is not subject to Anti-Money Laundering Measures Act, adopted on 27 March 2018 for not being at the moment the operations or transactions with virtual currencies within the typology o rules for the application of the AML Act, adopted on 31 December 2018, all based on the following considerations:

The BITCOIN was the first decentralized cryptocurrency or virtual currency conceived in 2009 by Satoshi Nakamoto. The term also applies to the protocol and the P2P network that supports it. Transactions in Bitcoin are carried out directly, without the need for an intermediary. Contrary to most currencies, Bitcoin is not backed by any government nor does it rely on trust in any central issuer, but uses a proof-of-work system to prevent double spending and reach consensus among all the nodes that comprise the net.
According to the GAFI Virtual Currencies, they report in June 2014, virtual currency is considered to be that which:

"It has a digital representation of value that can be used as a means of commerce and that works as a means of digital exchange, with a unit of account and deposit or reserve of value, but which does not have the status of legal tender in any jurisdiction".

Trinity Technologies EOOD carry out transactions with virtual currencies with individuals, who want to have cash through ATMs or buy cryptocurrencies through the different means of payment provided by the **Trinity Technologies EOOD** platform. These transactions for the purchase and sale of cryptocurrencies could be understood as a payment or electronic money activity and therefore be included in the type of obligatory

subjects of the Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018.

In order to qualify virtual currency as electronic money, we must go to Law 21/2011 of June 26 on electronic money, which defines it as:

"Any monetary value stored by electronic or magnetic means that represents a credit on the issuer, which is issued upon receipt of funds for the purpose of carrying out payment operations as defined in article 2.5 of Law 16/2009, of 13 of November, of payment services, and that it is accepted by a natural or legal person other than the issuer of electronic money. "

However, given the lack in cryptocurrencies of the support of a credit against the issuer, we must consider that they are not electronic money for the simple reason that that issuer does not exist.

Likewise, there are various international and European organizations that understand and consider that virtual currencies cannot be considered as current currency, neither electronic money or financial or payment instruments. Among these entities are:

a. The European Central Bank in its February 2015 Report on Virtual Currencies[1] and in its Opinion of October 12, 2016[2]

b. European Banking Authority in its opinion on virtual currencies of July 4, 2014[3] and in the Opinion of August 11 on the proposal of the EU Commission to bring virtual currencies to the scope of Directive (EU) 2015/849 (4AMLD)

c. FATF (Financial Action Task Force) or GAFI (Financial Action Task Force) in their June 2014 report[4] and in its June 2015 Guide[5]

[1] European Central Bank 2015 http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
[2] European Central Bank 2016
[3]EBA 2014 http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
[4] FATF 2014 https://www.fatf-gafi.org/documents/news/public-statement-june-2014.html
[5]FATF 2015 https://www.fatf-gafi.org/documents/news/public-statement-june-2015.htm

[7] Strategic Plan: http://ec.europa.eu/transparency/regdoc/rep/1/2016/ES/1-2016-50-ES-F1-1.PDF 8

On the other hand, after the terrorist attacks in Paris on November 13, 2015, the European Commission proposed on February 2, 2016 a Strategic Plan[6] to intensify the fight against the financing of terrorism in which it proposes to amend the Directive on the Prevention of Money Laundering[7], broadening the scope of application to include virtual currency exchange agencies or platforms and subject them to supervision in accordance with the legislation on money laundering and terrorist financing at the national level. In addition, it considers the application of the rules on licenses and supervision established by the Directive on payment services to be favorable, allowing better control and understanding of the market.

In this sense, the European position seems to be oriented towards the consideration of Virtual Currencies, as a means of payment, since in the Proposal for a Directive of the European Parliament and of the Council by which Directive (EU) 2015/849 is modified proposes to define virtual currency as:

«18)" virtual currencies ": digital representation of value not issued by a central bank or by a public authority, nor necessarily associated with a fiduciary currency, but accepted by natural or legal persons as a means of payment and that can be transferred, stored or traded electronically. ';

However, after the Opinion of the European Central Bank of October 12, 2016 to the aforementioned Directive proposal, the definition of virtual currency loses its status as a means of payment and is replaced as a means of exchange, being currently defined as:

«18) " virtual currencies": digital representation of value not issued by a central bank or by a public authority, nor associated with a legally established fiduciary currency that does not have the legal status of currency or money, but accepted by natural or legal persons as a medium of exchange and possibly also for other purposes and which can be transferred, stored or traded electronically.

The European Central Bank bases this change on the different uses that virtual currencies may have beyond the means of payment, such as a store of value, savings, investment, online casino, etc.

[8] Directive proposal: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52016PC0450&from=ES

6

7

Everything seems therefore to indicate, considering the current parliamentary procedures[8] and after the vote in the Council, that the definition of Virtual Currency in the future Fifth European Directive on Money Laundering will remain considered as a means of exchange and as electronic money or payment method.

On the other hand, although virtual currency cannot be considered as a legal currency or a financial instrument of payment, it can be defined as an electronic intangible asset with a unit of account that can be used in transactions of all kinds as a means of payment to the bearer and therefore such activity could be included in Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018.

Given that virtual currency is used as an electronic means of payment to bearer, and in particular it would be used by **Trinity Technologies EOOD** as a payment method for the provision of services for making cash available at the Hal-Cash Network ATMs, we could understand that Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, would be applicable. However, in the parliamentary consultation 184/47663 made to the European Governments on March 3, 2014 it is confirmed that for the moment the virtual currency Bitcoin cannot be considered as a means of payment to bearer[9].

Notwithstanding the foregoing, and despite the fact that the activity of **Trinity Technologies EOOD** It is not subject to Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, **Trinity Technologies EOOD** considers that the services it currently provides through the **Trinity Technologies EOOD** platform may constitute a tool for Money Laundering and therefore voluntarily submits to the application of said regulations.

In order to voluntarily comply with the obligations established by theAnti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, **Trinity Technologies EOOD** has requested the registration of the Representative of Bulgaria's National Investigation Service (NIS).

8

9

1.3. Anti-money laundering manual

Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, establishes that the obliged subject shall have a written program against money laundering and terrorist financing, the Manual for the Prevention of Money Laundering and Terrorism Financing, which will establish the policies, procedures and internal controls aimed at compliance with applicable legislation.

The purpose of this manual is to establish the rules and procedures necessary to comply with the provisions of current legislation in relation to the prevention and detection of money laundering, as well as to prevent it from being used in the financing of terrorism or other activities criminal.

This Prevention Manual must guarantee that **Trinity Technologies EOOD**:

- He knows his clients and has express client admission policies in place.
- It has staff responsible for compliance with the provisions against money laundering and terrorist financing.
- It complies with the requirements established by the laws for obtaining documents and the registration and communication of operations.
- Develops and implements appropriate control methods so that suspicious customer activity can be detected, immediately examine detected transactions, and take appropriate action.
- Report suspicious activities to the competent authorities in accordance with applicable law.
- It implements the necessary training programs on the prevention of money laundering and the financing of terrorism.
- It implements auditing and quality systems regarding its policies and procedures against money laundering and terrorist financing.

The Money Laundering Prevention Manual must be approved by the Internal Control organism on the Prevention of Money Laundering, and be publicized internally, informing employees of the controls and procedures implemented.

Employees who have information about operations, or activities classified as suspicious, are totally prohibited from transmitting it to any other company or person not related to the knowledge of the same, with the exception of the established Internal Control organism for prevention. Likewise, they have the duty of custody of said information diligently.

Trinity Technologies EOOD will proceed to the periodic verification and update of the manual, keeping a record to facilitate the monitoring of the changes that are incorporated into it.

2. INTERNATIONAL AND NATIONAL REGULATIONS

2.1. International regulations

The money laundering prevention policy emerged at the end of the 1980s as a reaction to the growing concern raised by financial crime derived from drug trafficking.

This concern makes existing international organizations react, such as the United Nations (UN), or the European Union (EU) itself, or encourages the creation of new organisms, such as the Financial Action Task Force (FATF).

In the regulatory field, the EU approved Directive 91/308 / EEC of the Council of the European Communities, of June 10, on the prevention of the use of the financial system for money laundering. The Directive urged Member States to prohibit money laundering and oblige the financial sector, including credit institutions and numerous other types of financial institutions, to identify their clients, keep the appropriate documents, establish internal procedures for training staff and to monitor money laundering, as well as to notify the competent authorities of any evidence of money laundering. This text was improved and substantially expanded in Directive 2001 / 97CE, of 4 December.

Finally, the so-called third directive, Directive 2005/60 / CE, was approved, repealing 91/308 / CEE, and which has been transposed into Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018.

Directive 2005/60 / EC or Third Directive, which basically incorporates the FATF Recommendations into Community law after its revision in 2003, is limited to establishing a general framework that must be, not only transposed, but completed by the states members, giving rise to notably more extensive and detailed national regulations, which means that the Directive does not establish a comprehensive framework for the prevention of money laundering and terrorist financing that is capable of being applied by obliged subjects without further specifications by the national legislator. On the other hand, the Third Directive is a minimum standard, as its Article 5 emphatically states, which must be reinforced or extended taking into account the specific risks existing in each Member State.

Directive 2005/60 / EC has been complemented by Directive 2006/70 / EC of the Commission, of August 1, 2006, which establishes provisions for the application of Directive 2005/60 / EC of the European Parliament and of the Council regarding, among other matters, the definition of "political people" and the technical criteria applicable in the simplified due diligence procedures with respect to the client.

The European Commission recognizes that the risks associated with money laundering are constantly evolving, which requires a periodic review of the legal framework. Therefore, in light of the recent review by the FATF (February 2012) of international standards and the implementation by the Commission of its own review process, it has prepared a report on the application of the Third Directive on money laundering. , and has started the process to approve the Fourth Directive.

Currently the Fifth Money Laundering Directive is in the final stage of approval pending approval by the European Commission and its publication in the TWELVE (Proposal for a Directive 2015 of the European Parliament and of the Council by which the Directive (EU) is modified / 849).

Given the lack of European regulations that regulate virtual currencies such as Bitcoin in the prevention of Money Laundering and terrorist financing, the following reports from various international organizations are also noteworthy:

- Report of the European Central Bank of February 2015 on Virtual Currencies, and the Report of October 12, 2016 in relation to the proposal for the fifth Money Laundering directive.
- FATF Report Virtual Currencies Key Definitions and Potential Risks (June 2014) FATF, Guidelines for a Risk-Based Approach (June 2015).

- European Banking Authority (EBA) “Opinion on Virtual Currencies” EBA / Op / 2014/08 4 July 2014 and “Opinion on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849.
- Strategic Plan for the fight against terrorism COM (2016) 50 final.
- Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. FIN-2013-G001.

2.2. National regulations

In the present Bulgarian legal framework, cryptocurrencies are still perceived, audited and declared before NRA (National Revenue Agency) as a financial asset. Their legal status got some development with the amendment to the Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, for not being at the moment the operations or transactions with virtual currencies within the typology of rules for the application of the AML Act, adopted on 31 December 2018. The principal points are:

• cryptocurrency-related service providers are among the obligated subjects under AML Act (Art. 4, p. 38 and 39), which means that they have to adjust their activity to the legal requirements for prevention against money laundering, otherwise sanctions may follow;

• for the very first time a legal definition of virtual currencies has been provided, namely “any digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically”;

• the registration regime with NRA (National Revenue Agency) is set in place as mandatory for some cryptocurrency-related service providers (those under the AML Act).

In August 2020, the Ministry of Finance issued Ordinance No. N-9 from 07.08.2020 setting the terms and procedure for entry into a public register held by NRA. Each register entry is conducted ex officio by NRA and

before the start of the cryptocurrency-related activity by the respective person, be it natural persons, including sole proprietors, legal persons like companies as well as other legal entities.

Bulgaria is a member of MONEYVAL. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards - FATF recommendations. One of the most fundamental FATF standards is a requirement for countries to identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Identifying, assessing, and understanding ML/TF risks is an essential part of the implementation and development of a national anti-money laundering / countering the financing of terrorism (AML/CFT) regime, which includes laws, regulations, enforcement and other measures to mitigate ML/TF risks. It assists in the prioritization and efficient allocation of resources by authorities.

2.3. Obligations in the regulations on the prevention of money laundering

According to Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, for not being at the moment the operations or transactions with virtual currencies within the typology o rules for the application of the AML Act, adopted on 31 December 2018, the obligated subjects have to comply with the following obligations:

1. Regarding customers and their businesses

Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, distinguishes three groups of due diligence measures regarding clients and their businesses: normal, simplified and reinforced measures.

Within the normal measures, the obligations are established to formally identify the client, identify the beneficial owner in the cases where appropriate, obtain information on the purpose and nature of the business relationship, and continuously monitor the business relationship.

Inside that group of simplified measures establishes a series of cases in which obligated subjects are authorized not to apply the above measures to certain clients, with respect to which it is considered that they carry a low risk of money laundering. Likewise, simplified due diligence measures are established for certain products or operations, establishing quantitative limits in some cases. The Regulation has authorized the application of other simplified due diligence measures, with respect to customers, as well as products and operations that carry a low risk of money laundering.

Finally, a series of reinforced due diligence measures are established, in both, the Law and the Regulations, in cases that may present a greater risk for money laundering, such as private banking activity, remittance services money, foreign currency exchange operations, business relationships and remote operations, cross-border banking correspondent relationships, relationships with people with public responsibility, or products or operations conducive to anonymity and new technological developments.

2. Communication of operations and collaboration with NIS

Included in this group are the obligations to carry out an examination of suspicious transactions, report them to NIS, refrain from executing suspicious transactions or establish relationships with the client, and not communicate the submission of information to NIS.

Also included are the obligation of systematic communication of obligations by certain obliged subjects (for an amount greater than a certain amount) and collaboration with the NIS, to:

- Provide documentation and information that is requested.
- Attend to your needs.
- Have the duty of reservation regarding the communications received.
- Facilitate supervision and inspection activities.
- Attend the requirements made on corrective measures after an inspection.
- Have the duty of reserve regarding the reports or requirements requested.

3. Conservation of documentation

The documentation in which the fulfillment of the obligations is formalized shall be kept for a minimum period of ten years.

4. Internal control

Within the internal control measures,Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018 establishes the following obligations:

- Written approval and application of appropriate policies and procedures.
- Written approval of the express client admission policy.
- Appointment of a representative before the NIS.
- Creation of an internal control body.
- Approval of a manual for the prevention of money laundering

The aforementioned internal control measures may be established at the group level, according to the group definition established in article 42 of the Commercial Code, provided that said decision is communicated to the NIS, specifying the obligated subjects within the group's structure.

These formal and procedural obligations are simplified for obligated subjects who employ less than 10 people, and whose annual volume of operations does not exceed 2 million euros.

5. Training and protection of employees

Obligated subjects will adopt the appropriate measures so that their employees are aware of the requirements derived from the regulations on the prevention of money laundering and will adopt the appropriate measures to maintain the confidentiality of the identity of the employees, managers or agents who have made a communication to the internal control bodies.

6. To submit to the examination of an external expert (auditor)

The results of the examination will be consigned in a written report that will describe in detail the existing internal control measures, will assess their operational effectiveness and will propose, where appropriate, possible rectifications or improvements.

This obligation is not required of individual entrepreneurs or professionals.

7. Declaration of fund movements

Individuals who, acting on their own or third parties, carry out the following movements must submit a prior declaration:

- exit or entry into national territory:
- of payment method for an amount equal to or greater than 10,000 euros or the equivalent in foreign currency.
- bearer negotiable instruments, including monetary instruments such as traveler's checks, negotiable instruments, including checks, promissory notes and money orders, whether they are made out to the bearer, endorsed without restriction, made out to the order of a fictitious beneficiary or otherwise in By virtue of which the ownership of the same is transmitted upon delivery, and incomplete instruments, including checks, promissory notes and payment orders, signed but with omission of the beneficiary's name.
- movements by national territory of means of payment for an amount equal to or greater than 100,000 euros or its equivalent in foreign currency. For these purposes, movement shall be understood to be any change of place or position that occurs outside the domicile of the bearer of the means of payment.

8. Against the financing of terrorism

Measures against the financing of terrorism, such as the freezing and blocking of funds and economic resources, are regulated in the Law, and developed in the regulations.

3. CONCEPT OF MONEY LAUNDERING AND TERRORISM FINANCING

3.1. Money laundering concept

The following activities will be considered money laundering:

- The conversion or transfer of goods, with the knowledge that the mentioned goods come from a criminal activity or from participation in a criminal activity, with the purpose of hiding or concealing the illicit origin of the goods or helping people who are involved to avoid the legal consequences of their actions.
- The concealment of the nature, origin, location, disposition, movement or real ownership of goods or rights to goods, with the knowledge that the aforementioned goods come from a criminal activity or participation in an activity criminal.
- The acquisition, possession or use of goods, with the knowledge, at the time of receipt, that they come from a criminal activity or from participation in a criminal activity.
- Participation in any of the activities mentioned in the previous letters, the association to commit this type of act, the attempts to perpetrate them and the fact of helping, instigating or advising someone to carry them out or facilitate their execution.

It will be considered that there is money laundering even if the activities that have generated the goods had been developed in the territory of another State.

Assets from criminal activity shall be understood to be all types of assets, the acquisition or possession of those that have their origin in a crime, both material and immaterial, movable or immovable, tangible or intangible, as well as documents or legal instruments independently of its form, including electronic or digital, that prove the ownership of the aforementioned assets or a right over them, including the fee defrauded in the case of crimes against the Public Treasury.

3.2. Terrorism Financing Concept

Terrorism financing shall be understood as the supply, deposit, distribution or collection of funds or goods, by any means, directly or indirectly, with the intention of using them or with the knowledge that they will be used, in whole or in part, for the commission of any of the crimes of terrorism typified in the Penal Code. Financing of terrorism will be considered to exist even if the supply or collection of funds or goods has taken place in the territory of another State.

4. PROPPER POLICIES AND PROCEDURES

Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018 establishes that the obliged subjects, with the exceptions determined by regulation, shall approve in writing and apply adequate policies and procedures in matters of due diligence, information, document preservation, internal control, risk assessment and management, guarantee compliance with the relevant provisions and communication, in order to prevent and prevent operations related to money laundering or terrorist financing.

In practice, the appropriate policies and procedures will materialize in the following actions:

4.1. Departments of Trinity Technologies EOOD that may be affected by the obligations established in the regulations on the prevention of money laundering

The following departments or work centers are affected by the obligations of the regulation on money laundering:

- **Departments:**

- System Departament.
- Operations Support Department.
- Finance / Support Department.
- Administration Department.

- **Workplace:**

- 2v Topli dol St, ap 16, Sofia, Bulgaria, 1680.

4.2. Trinity Technologies EOOD Departments that have to fulfill each of the obligations

- Due diligence measures with clients: Dpt. Financial / Support / Administration.
- Detection and analysis of suspicious operations: Dpt. Systems.
- Communication and collaboration with NIS: Dpt. Financial.
- Document preservation: Dpt. Systems.
- Training of managers and employees: Dpt. Financial.

4.3. Coordination rules and information transmission channels between them

The fundamental channels for the transmission of information between the departments will be the corporate email, the telephone and the quarterly or emergency meetings held in situations of suspicion of Money Laundering.

5. POLICIES FOR ADMISSION, KNOWLEDGE OF THE CLIENT, AND MONITORING OF YOUR BUSINESS

5.1. Objectives of the admission and knowledge of the client policies

One of the fundamental requirements in the fight against money laundering is the identification and knowledge of customers, regular or not.

Following the content of the EU Directives, distinguishes three groups of due diligence measures regarding clients and their businesses: normal, simplified and reinforced measures.

A structured due diligence procedure should include the periodic updating of the required documentation and information. The update will be, in any case, mandatory when there is a relevant change in the client's activity that could influence their risk profile.

Within the normal measures, the obligations are established to formally identify the client, identify the beneficial owner in the cases where appropriate, obtain information on the purpose and nature of the business relationship, and continuously monitor the business relationship. .

The client admission policy must establish a precise description of the clients that potentially may pose a risk higher than the average by regulatory provision or because it is thus deduced from the risk analysis, and the measures to be adopted to mitigate it, including, where appropriate, the refusal to establish business relationships or carry out operations or the termination of the business relationship.

In this line, the policy of admission and knowledge of the client, which is set out below, incorporates the procedures and internal controls that guarantee an effective and complete knowledge of the clients and their activities, by the employees, in order to:

- Comply with the Client Identification Policy when a relationship is initiated or an operation is carried out, guaranteeing that operations are not carried out with individuals or entities whose identities cannot be verified, that do not provide necessary information or that have provided false or incoherent information, or especially checking if a client is within the public lists issued by the European Union and the UN through their different regulations.
- Execute active "knowledge of the customer" policies, confirming and documenting the true identity of customers who maintain any type of business relationship.
- Confirm and document any additional information about the client, in accordance with the assessment of the risks of money laundering and the financing of terrorism, especially monitoring those clients who are considered to be at higher risk, reporting any modification or significant movement to the internal control body.
- Analyze in detail any operation / client that shows suspicions or indications of a possible link to money laundering, communicating it as soon as the internal control body.

- Inform the internal control body about the possibility of exempting certain clients from the obligation to report their operations to The Government of Bulgaria has ruled a low level of terrorist threat in Bulgarian National Revenue Agency (BNRA) when their activity and origin of the funds is widely known.

The policy in relation to clients is based on the following fundamental pillars:

- Identification and knowledge of the client.
- Customer admission policies.
- Continuous monitoring of business.

For this, it is necessary to claim and obtain information from clients about the client's activity or operations, and adopt measures aimed at reasonably verifying the veracity of said information, according to the level of risk that has been determined for the client.

5.2. Identification and knowledge of the client

Trinity Technologies EOOD You must correctly identify each customer with a dual purpose:

- Comply with the legal and internal regulations regarding the identification and knowledge of the client.
- To be able to discriminate if you belong to any of the groups affected by the customer acceptance policy.

The actions to be carried out are the following:

5.2.1. ID

In compliance **Trinity Technologies EOOD** will maintain business relationships or carry out operations with individuals or legal entities that have not been duly identified, as long as the limit of operations is greater than 1,000 euros.

Registration on the Platform

Notwithstanding the foregoing, **Trinity Technologies EOOD** services require prior registration and acceptance of the platform's terms and conditions, regardless of the amount of the transaction for which the following information must be provided:

- Name and surname.
- Email address.
- Password.
- Image of the DNI or passport on the front and back.
- Selfie: where the Client is seen holding their identity document next to a piece of paper where it says "https://crypto-trinity.com/" and the date or power of attorney of the representative in the case of a legal entity.
- Mobile phone number.

Once the information is received, the information provided by the User is manually verified and validated, verifying the authenticity of the photographs and documents provided, as well as their nationality.

Then, an additional verification (AFSCORING ****) is carried out by contacting the User by phone, including the following questions:

1. Are you aware that you buy cryptocurrencies at **Trinity Technologies EOOD**?
2. Have you registered with **Trinity Technologies EOOD** freely and voluntarily or have you been asked to do so?
3. The purchases you will do at **Trinity Technologies EOOD** are also voluntary and conscious, right?
4. Additionally, the user is asked about their knowledge about the ecosystem of cryptocurrencies and the risk involved in operating with them (price volatility, etc.).

If everything is correct, the Client will receive an email to confirm their account.

Subsequently, in the cases in which there are doubts about the validity of the DNI or the investigation procedures carried out by **Trinity Technologies EOOD** regarding the IP, cookies, country and mobile phone made are doubtful, additional information is requested from the client:

- Invoice that shows a match between the address and ID.
- Selfie holding bank card.

Once the registration process is authorized, the user must pass the identification and knowledge process of Clients to be able to make purchases and sales of cryptocurrencies in accordance with the procedure established on the web.

Once the Client is registered, his formal identification is carried out. Clients must prove their identity by means of one of the following reliable documents, which must be current and digitized:

A) Natural persons

- **Natural persons of Bulgarian nationality:**

- The National Identity Document.

- **Natural persons of foreign nationality:**

- The Residence Card.
- The Foreigner Identity Card.
- The Passport or, in the case of citizens of the European Union or the European Economic Area, the document, letter or official personal identity card issued by the authorities of origin.
- The identity document issued by the Ministry of Foreign Affairs and Cooperation for the personnel of the diplomatic and consular representations of third countries in Bulgaria will also be a valid document for the identification of foreigners.

Exceptionally, other personal identity documents issued by a government authority may be accepted as long as they enjoy adequate guarantees of authenticity and include a photograph of the holder.

B) Legal persons

- Public deed of incorporation containing its company name, legal form, address, the identity of its administrators, statutes and tax identification number. (In the case of legal persons of Bulgarian nationality, it will be admissible, for the purposes of formal identification, certification from the provincial Mercantile Registry, provided by the client or obtained through telematic consultation).
- Deeds of empowerment of the people who act on their behalf, as well as their identification documents.

In case of legal or voluntary representation:

- Deeds of empowerment of the people acting on their behalf, as well as identification documents of the representative and the person or entity represented. (It will be admissible the verification by certification of the provincial Mercantile Registry, provided by the client, or obtained through telematic consultation)

In entities without legal personality:

- **They carry out business activity:**

- Proof of identity documents are provided for all participants.

- **They do not carry out business activity:**

- Identification document of the person acting on behalf of the entity is provided.

In the customer identification phase, the following situations involve alarms that must be resolved before admission:

- The identity document of the examined customer appears to be a forgery or is found to be adulterated.
- The client is reluctant or refuses to supply the required information.

- The client asks many questions about the money laundering controls or the limits of the declaration of funds.

For the purposes of compliance with the Identification Duty, the customer identification templates established as Annex 12.4.1 for natural persons and 12.4.2 for legal persons included in this Manual will be used.

5.2.2. Identification of the beneficial owner

Trinity Technologies EOOD will proceed to identify the beneficial owner and will adopt appropriate measures in order to verify their identity prior to the establishment of business relationships or the execution of any operations.

For it, **Trinity Technologies EOOD** will adopt the necessary measures to obtain information from customers, to determine whether they act on their own account or on behalf of third parties. In addition, in the case of companies or other legal entities, the statement on the real ownership of the operation will be collected by means of a responsible declaration of the client (natural persons with direct or indirect possession or control of 25% or more of the capital or of the voting rights of a client that is a legal entity or that by other means exercises control of its management).

In relation to the identification of the beneficial owner, article 9.1 of the Regulation provides that the identification and verification of the identity of the beneficial owner may be carried out, in general, by means of a responsible declaration of the client or of the person assigned to represent the company. legal person, for these purposes, the administrators of the companies or other legal persons must obtain and maintain adequate, accurate and up-to-date information on the beneficial ownership of the same.

Trinity Technologies EOOD requires all clients to make a responsible declaration in accordance with the template included as Annex 12.4.3, and verifies that the information agrees with that which is registered in the corresponding registry.

However, it will be mandatory to obtain additional documentation or information from independent reliable sources when the Client, the beneficial owner, the business relationship or the operation present risks above

the average and, in any case, when there are indications that the identity of the real owner declared by the Client is not exact or truthful, or when there are circumstances that determine the special examination or communication by indication.

Information will be collected from Clients to determine whether they act on their own account or on behalf of third parties. When there is any doubt about whether the owner is not acting on his own account, before carrying out any operation, he must have all the information necessary to determine who is the real owner. When there are indications or certainty that Clients are not acting on their own account, precise information will be collected in order to know the identity of the people on whose behalf they act, which may be accredited as follows:

- Newly constituted companies, the structure of the capital stock may be accredited with the data contained in the deed, unless the Client accredits other more updated data.
- Companies incorporated more than one year ago, the accreditation may be carried out from the corporate tax, the annual accounts report or by providing certification from the secretary of the Board of Directors or the registration authority.

In the case of companies whose shares are represented by bearer titles, a certification from the Secretary of the Board of Directors or the main governing body will be required on the ownership or control structure, or a public document containing this information.

In the case of legal persons constituted or resident in tax havens or non-cooperating countries and territories, a certification of the composition of their administrative bodies or main governing body will always be obtained, stating the identification of the partners they own or control, Directly or indirectly, shares of any type or voting rights greater than 25% of the total.

5.2.3. Purpose or nature of the client's business

Obligated subjects will collect information from their clients in order to know the nature of their professional or business activity prior to the start of the business relationship.

Additionally, the veracity of the activities declared by the Client must be verified when there are risks above the average, because this is established by regulatory provision or because it is derived from the risk analysis and when the operations carried out do not correspond to the activity that has declared or with the operational history that exists.

The verifications will be based on obtaining from the Clients documents that are related to the declared activity or on obtaining information from sources outside the same or even through face-to-face visits to their declared offices, warehouses or premises, leaving a written record of the result. of said visit.

Trinity Technologies EOOD will proceed to identify the client, collecting, in accordance with Annex 12.4, all the necessary information that allows them to obtain an understanding of their economic activity.

In the case of natural persons, information will be collected on the exercise by the client, or their relatives or close friends, of important public functions abroad and in Bulgaria, currently, or in the previous two years.

According to Annex 12.4, among the documents that could be requested from the client to fulfill this obligation, the following can be indicated:

A) Individual clients:

- Payroll.
- Payment receipts for the self-employed Social Security regime.
- Declaration of the Tax on Economic Activities.
- VAT returns (monthly or quarterly, and the annual summary statement).
- Personal income tax return.
- Documentary justification in the event that they claim to depend on other family members.

B) Legal entity clients:

- VAT returns (monthly or quarterly, and the annual summary statement)
- Corporate Tax Declaration.
- Annual accounts presented in the Mercantile Registry.

5.2.4. Conservation of documentation and formation of the file

A copy of all the documentation related to the identification of clients, including the Client and Risk Identification Forms in Annex 12.4, must be duly filed and kept in a special file and kept for a period of 10 years.

5.3. Client admission policy

5.3.1. Objective

The admission policy includes a description of those types of clients that could present a higher risk than the average, depending on the activity sector to which they belong, the origin or residence of these clients, or any other information from which they are arranged.

The admission policy must be applied to all clients who exceed the economic and temporal limits of operations established in this Manual.

The risks inherent in money laundering or terrorist financing can be managed in a more effective and efficient way if the potential risk associated with the different types of clients and their operations is previously known. To do this, the factors that allow weighing the risk of each type of client must be taken into account, namely:

- The nature of the products and services offered by the entrepreneur / professional.
- The intended use of the products and services by the customer.
- The environment in which the entrepreneur / professional and their clients are located.

Identifying the clients by risk levels will allow the professional to design and implement measures and controls to mitigate said risks. In the same way, it will allow you to focus on the customers and transactions that present the highest risk.

5.3.2. Customer segmentation based on money laundering risk

Trinity Technologies EOOD has established a procedure, based on the consideration of its own business risk and the services it offers, which provides an adequate framework that allows segmenting its own clients by levels of risk of money laundering or financing of terrorism.

The procedure for classifying customer risk has the following characteristics:

5.3.2.1. Goals

- Systematically classify clients according to the degree of risk they present of committing the crime of money laundering and terrorist financing.
- Identify high-risk customers.
- Establish the pertinent controls that allow the institution to mitigate the inherent risk of the high-risk client.
- Give priority to monitoring the operations of these clients.

In some cases, the risk may only become apparent once the client has commenced operations, making it necessary for the monitoring of the client's operations to be a fundamental component of the risk-based approach.

5.3.2.2. Risk factors

The main risk factors used in the classification system, and which are incorporated into a Client Risk Sheet to identify those who may have a high risk of money laundering, are the following:

A) Seniority level of the client

The new customer, for whom no prior information is available, is considered to be at higher risk. The older the relationship, the risk is lower.

B) Geographic, international and national risk

The international geographic risk of the client is determined, taking into account whether the location of its registered office, and the territories in which it operates, are included in the lists of tax havens or non-cooperating territories.

Nationality:

- Bulgaria (1 point).
- Countries of the European Union and OECD (2 points).
- Other countries (3 points).
- Tax havens and countries identified by the FATF and the European Commission, as indicated in Annex 12.7 (4 points).

C) Residence

Residence in Bulgaria (1 point), in other countries (3 points).

Customers who exceed five points will be considered as Customers who present a higher than average risk.

D) Risk of the client's economic activity / business

It is considered as a risk factor that the client has the status of an obligated subject in theAnti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, or that they carry out any of the activities mentioned in the types of money laundering of the NIS. **Trinity Technologies EOOD** you may consider including other suspicious activities, based on existing circumstances, such as the client's business activity, or that of the client's clients.

E) Background of the client, in the case of natural persons

Trinity Technologies EOOD applies reinforced due diligence measures in business relationships or operations of persons with public responsibility, which are those individuals who perform or have performed important

public functions in other Member States of the European Union or in third countries, as well as their family members, more relatives and people recognized as close friends.

Trinity Technologies EOOD has verified that the client is not included in any list of sanctions of international organizations identified in Annex 12.8.

5.3.2.3. Risk sheet for customer risk classification

Trinity Technologies EOOD has a Client Risk Form in accordance with Annex 12.9, which integrates the risk factors previously contemplated and assigns, in accordance with the information submitted by the client, one of the following risk categories:

- RISK FREE
- AVERAGE RISK
- HIGH RISK

In the process of registering a new client, you must include among your data, as additional information, the classification of your risk (No risk, Average or High), according to the result obtained in the Risk Sheet.

The form has been stored in the client's file.

5.3.3. Client acceptance procedure

Depending on the risk of money laundering, the following categories of clients are established to whom a different client acceptance procedure will be applied.

A) Clients without risk of laundering

The following will be included in this group:

- Those that do not exceed the quantitative limits of 1,000 euros in operations linked to each other in reduced periods of time.
- That they provide all the identification documentation that is required of them.

- That they are not within the sections listed below under the headings "Customers with average risk level" or "High risk customers".
- That they are not on the international lists of people, groups and entities linked to the financing of terrorism.
- That, once the identification documentation they provide has been analyzed, they are considered suitable by **Trinity Technologies EOOD** after analyzing the documentation provided. If from said analysis it is possible to perfectly identify the Client, as well as reasonably determine that their funds and assets are legitimate, we will be in front of a suitable or acceptable Client.

Once a Client is accepted, the relationship with the same will end whenever the same refuses, unjustifiably, to provide the required data.

The relationship with a Client must also be terminated, when the operation carried out is not in accordance with its transactional profile, and there is evidence of its possible connection with money laundering or terrorist financing.

However, before ending the relationship with a Client, the reasons that lead to said decision must be documented.

The relationship with a Client must be subject to review whenever it is suspected that they may be involved in criminal activity, and when it appears on an international list of suspects.

When unsolvable identification problems arise once a Client has been accepted, the contractual relationship should, if possible, be canceled, assessing the possibility of communicating this fact to NIS.

Process: the client is supported without having to perform any additional operations. The client's identification card will not be completed and will be filed in your file.

B) Customers with average risk level

Clients who do not present a high risk or have been accepted are included in this category.

Process: in the obligation of continuous monitoring of the client's operations / business, verifications will be made of the situations or operations that could pose a risk of money laundering.

C) Clients with a high level of risk

The following clients are included in this group:

A) People who reside, have funds or regularly operate in countries with inadequate levels of controls in the prevention of money laundering (tax havens and non-cooperating territories).

B) People involved in business activities or sectors recognized as likely to be used for money laundering, such as:

- sale of imported vehicles.
- importation of scrap metal or other merchandise whose origin / economic purpose is difficult to determine.
- customers related to the production or distribution of weapons and other military products.
- clients that engage in transactional activities on behalf of third parties.
- Clients whose commercial activity is the exploitation of: casinos, gaming machines, betting or other games of chance, who have the mandatory administrative authorization to operate.
- Establishments that carry out the activity of currency or currency exchange and / or transfer management, which prove the existence of the appropriate administrative authorization, and the adequate control procedures regarding the prevention of money laundering.
- Clients who are directors, shareholders or owners of exchange houses, money transmitters, casinos, betting companies or other similar entities.
- Clients who are people with public responsibility.
- Companies whose capital is not sufficient to carry out the activities it projected, unless its sources of financing are known.

Process: for clients that obtain a High Risk classification, the following measures and controls must be applied:

Controls at the beginning of the relationship:

High-risk clients will be asked for additional documentation on economic activity, such as:

- Document the main products or services you offer.
- Geographic coverage where it operates.
- Knowledge of your customers and suppliers.
- Number of clients it has and number of branches.
- If the client carries out a regulated activity, verify its records before the regulatory body, and verify if it complies with that established by the same.

The Control organism will make the final decision regarding the admission or not of a specific client.

Customer follow-up controls:

It will be periodically verified that the available information of the client agrees with the profile declared at the beginning of the relationship. Otherwise, the situation must be documented and recorded in the file.

Review of high risk clients by the internal control body.

The files of clients classified as High Risk must be sent to the Internal Control Body, in order to evaluate whether the established controls were applied. If there are breaches in them, a report is made in order to correct them.

5.3.4. Clients excluded from acceptance

The Regulations of the prevention of money laundering and terrorist financing establishes that in no case, the obliged subjects will maintain business relationships or carry out operations with natural or legal persons that have not been duly identified, as long as the limit of operations is greater than 1,000 euros.

For all normal due diligence measures (formally identify the client, identify the beneficial owner in the cases where appropriate, obtain information on the purpose and nature of the business relationship, and make continuous monitoring of the business relationship), that business relationships will not be established or operations will be carried out when these measures cannot be applied. When the impossibility is appreciated in the course of the business relationship, the obligated subjects will put an end to it, proceeding to carry out a special examination of the operation, reviewing the results of the same in writing.

For reasons of controlling the risk of money laundering, the following clients will not be accepted:

A) People who have not been able to be identified with the documents required in the regulations.

B) People with whom there are discrepancies between the data provided by the client and other accessible information or in the possession of the obliged subject.

C) People on whom some information is available that may be related to criminal activities.

D) People who have businesses whose nature makes it impossible to verify the legitimacy of the activities or the origin of the funds.

E) Legal persons whose shareholding or control structure cannot be determined.

F) People who refuse to provide the information or documentation required for their identification or, where appropriate, to justify their economic activity or the origin of the funds, or the purpose and nature of the business relationship.

G) People who provide documents of doubtful legality, legitimacy or manipulation.

H) People included in any of the official sanctions lists.

I) Clients whose commercial activity is the exploitation of: casinos, gaming machines, betting or other games of chance, who do not have the mandatory administrative authorization to operate.

J) Clients who, due to their circumstances, do not appear to be carrying out professional or business activities, or have means compatible with the operation they intend to carry out

K) Clients who, because they come from remote jurisdictions, make it impossible to comply with the obligations imposed by the Law.

5.4. Policy of continuous monitoring of customer operations or businesses

5.4.1. Introduction

On continuous monitoring of the business relationship, establish the following:

Obliged subjects will apply continuous monitoring measures to the business relationship, including scrutiny of the operations carried out throughout said relationship in order to guarantee that they coincide with the knowledge that the obligated subject has of the client and of their business profile and of risk, including the origin of funds and ensure that the documents, data and information available are up-to-date and current.

Thus, the knowledge of the client does not end with their identification, but requires knowledge of the framework in which they operate, and careful monitoring of the evolution of their activities.

In due diligence measures with clients, employees who, due to their function, have "knowledge of the client" due to the personalized and close treatment they maintain with them, or because they know their operations, are of special importance. These employees can deal directly with the client at the initial moment of establishing the specific business relationship or operation, or later, for the duration of the business relationship.

5.4.2. Updating of customer knowledge and verification process

The knowledge of the client, and the verification of the veracity of the information provided by him, are obligations that remain over time and that must be periodically updated; it is not enough to obtain it at the beginning of business relationships.

The data and activities declared by the client and incorporated into their Identification Card must be reasonably verified in order to guarantee their veracity. Customers' operations should also be monitored, trying to detect if there are variations in their behavior that are inconsistent with the declared activities. If so, it would be a potentially suspicious situation of being linked to money laundering.

A series of measures are detailed below, the application of which makes it possible to reasonably verify the veracity or otherwise of the information provided by customers. Although it is true that not all the measures can be applied in all cases, the aim is to offer a wide enough range to be able to apply, in all cases, some of them:

- After the start of the business relationship, and during the first months, periodically check that the operations and activity of the Client is consistent with the activity stated.
- Consult the commercial reports available.
- When they refer to commercial companies, which are new clients and their administrators and / or partners are not known, the commercial report on the company and other companies where administrators and / or partners hold social positions should be consulted as soon as possible.
- When they refer to non-profit NGOs, Associations and Foundations:

- Check a public list of NGOs, Associations or Foundations where the client appears (Ministry of Culture, List of Autonomous Communities, etc.).
- Check the payment of public subsidies.
- Check the existence of bills for water, electricity, telephone, municipal taxes, etc.
- Check the existence of a social or local headquarters for activities.
- Analyze if there is any relationship between the members of the government team.
- Regarding the disposition of the funds, check that payments are observed to subjects or situations that are consistent with the declared activity. Pay special attention to cases in which the funds are mainly available in cash.

The following are considered alarm situations that require express verification:

- New customer who immediately begins to carry out high-value cash movement operations that are not justified by the declared activity.
- The amounts of the client's operations do not respond with their proven economic level.
- The address provided by the client is not correct.
- There are difficulties in knowing the professional or business activity carried out by the client.

5.4.3. Deadlines for updating the information

For high-risk clients, the updating of the information that supports the client's knowledge and the verification processes thereof must be carried out at least every 12 months.

For the rest of the clients, the period for updating the information on the knowledge of the client will remain open, as long as no indications of possible links with money laundering are detected, since if this is the case, the measures aimed at deepening the knowledge of the client and verifying the information / documentation provided.

6. DETECTION OF SUSPICIOUS OPERATIONS AND COMMUNICATION TO THE NIS

6.1. Alert system

All departments involved in the prevention of money laundering will put into practice, in accordance with the procedures established in each case, methods of analysis and adequate control of customer operations, specified in current regulations, so that during the relationship with the client possible:

- Detecting suspicious transactions.
- Analyze operations.
- Inform the authorities, in accordance with the applicable legislation.
- Collaborate with the commission for the prevention of money laundering and monetary offenses.

To detect suspicious transactions, **Trinity Technologies EOOD** has established an alert system regarding operations that, by their nature, could (because they are complex, unusual or without an apparent economic or legal purpose, or because they show signs of simulation or fraud) be related to the BC / FT.

The OCIC will be responsible for analyzing the operations that it considers likely to be related to money laundering and terrorist financing.

The alert system of **Trinity Technologies EOOD** will be based on the following:

- Coincidences in the international lists of people, groups and entities linked to the financing of terrorism or in the lists of Sanctions indicated in this Manual;
- Operational with natural or legal persons that are residents, or act on their behalf, in territories or countries listed in Annex VII of this Manual;
- Operations that imply transfers of funds to or from the territories or countries mentioned in the previous point, regardless of the residence of the intervening persons;
- Operations whose amount exceeds 100,000 euros or its equivalent in foreign currency;
- Operations that, in the opinion of the OCIC, present a high fractionation;
- High risk clients or attempted operations by excluded Clients, in the terms described in this Manual.

Trinity Technologies EOOD does not carry out operations that involve the physical movement of metallic currency, banknotes, traveler's checks, checks or other bearer documents issued by credit institutions for an amount greater than 30,000 euros per month or the equivalent in foreign currency.

Finally, we must point out the commitment assumed by the OCIC to analyze, for the purposes of compliance withAnti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, the eventual connection of its Clients with the financing of terrorism.

These alerts will be reviewed every six months in order to guarantee their permanent adaptation to the characteristics and level of risk of its operations.

6.2. Suspicious transaction detection

In the framework of detecting operations with indications, the obligated subjects must have a catalog or register of types of operations related to the PBC / FT that, depending on the activity carried out and the obligated subject's own experience, have occurred in the course of the business relationship. Each of these types of risk operations must present and describe a specific pattern and a series of concurrent risk elements, as well as the actions to be taken in the event of detecting attempts to carry out said operations, basically abstention from execution. and, where appropriate, communication to the NIS.

The Regulation of the Laws provides that the obliged subjects shall internally disseminate a list of operations that may be related to money laundering or terrorist financing.

Trinity Technologies EOOD In application of this precept, it has communicated to the directors, employees and agents, via email, the catalog of suspicious transactions identified in Annex 12.6 of this manual.

Trinity Technologies EOOD has a procedure that establishes the communication of suspicious transactions to the NIS, as long as:

- Are related to funds originating from criminal activities or are intended to hide funds or assets originated by these activities.

- They do not have a commercial purpose or there is no reasonable explanation for such operations, after examining the known facts, including the background and the possible objective of the operations.

Annex 12.10 includes the suspicious operation model that they must fill out **Trinity Technologies EOOD** in the case of detecting suspicious transactions

6.3. Internal communication

The regulations establish that the obliged subjects will establish a channel of communication with the internal control organism, with precise instructions to the managers, employees and agents on how to proceed in case of detecting any fact or operation that could be related to money laundering or the financing of terrorism.

Trinity Technologies EOOD it has rules and procedures that establish the communication of suspicious operations to the Internal Control organ, and, when they consider it, the communication of suspicious operations to the NIS, provided that:

- Are related to funds originating from criminal activities or are intended to hide funds or assets originated by these activities.
- They do not have a commercial purpose or there is no reasonable explanation for such operations, after examining the known facts, including the background and the possible objective of the operations.

Annex 12.10 includes the suspicious transaction model of the employees and managers of the **Trinity Technologies EOOD** in the case of detecting suspicious transactions.

6.3.1. Obligation of staff

All employees, within their functions, have the obligation to examine with special attention any operation, regardless of its amount, that may have indications of being related to money laundering or terrorist financing, communicating it to the Control organism so that The latter decides whether to communicate it to the NIS.

The internal procedure for reporting suspicious transactions by staff and managers to the internal control organism is included in Annex 12.10 of this manual, and will be sent by email to the Internal Control Body.

6.3.2. Communication channels

The employee who performs or detects a doubtful operation will immediately communicate this situation via email to the person in charge of the Internal organism, which is the organism responsible for the analysis. This organism will examine the circumstances, trying to determine if it is indeed suspicious.

Once the communication to the Control organism has been made, the communicator will be exempt from responsibility. Whatever the criteria adopted by the Control organism, with respect to the communications made, the communicator will be informed of the course that is given.

6.4. Actions of the internal control organism

The internal organism will carry out the following actions:

a) Reception of the communication, which must be registered.
b) Examination of the circumstances.
c) Request for additional information, if deemed necessary.
d) Final decision, which will appear in a written report, and which will state the reasons for said decision.
e) Control of compliance with the decisions taken.

The internal control organism will communicate, by email, information to the staff and managers of the course given to its communication.

In the event that, after a period of twenty business days, the communicator has not received any response on the status of his communication, he may choose to communicate directly to NIS the facts that had previously been revealed to the Control organism with indication to the latter that he makes such direct communication.

When communications are made about suspicious operations or activities to the internal prevention organism, it will be totally prohibited to provide any information both internally and externally about the clients or operations to which the information refers.

6.5. Analysis of operations

The Control organism will carry out additional investigative steps on the operations detected with the maximum depth and speed possible, by obtaining all the information and documentation available, and the global investigation of the clients' operations, considering the possible relationship with other clients or sectors of activity.

In view of all the documentation collected, the Control organism will decide on the origin of its communication to NIS. If so, the operation will be communicated, together with the documentation that supports the steps taken.

The electronic communication form or means provided in each case by the NIS will be used for this.

The analysis of risk operations (abnormal, unusual or potentially constituting an indication or certainty), the deliberations held, as well as those communicated to NIS, will be recorded. In particular, these records will refer to each operation studied, client, identification, reason for the alert, extension of data carried out if necessary, decision made to refer or file and reason, as well as any other data or antecedent that, at the view of the specific operation, it will be relevant for its evaluation.

6.6. Communication to NIS of operations

Trinity Technologies EOOD shall communicate, on its own initiative, to NIS any fact or operation, even the mere attempt, regarding which, after the special examination, there is an indication or certainty that it is related to money laundering or terrorist financing.

6.6.1. Operations to be reported

In particular, **Trinity Technologies EOOD** will notify the Executive Service of the Commission of operations that show an ostensible lack of correspondence with the nature, volume of activity or operational history of

the clients, provided that in the special examination provided for in the preceding article there is no economic, professional or professional justification business to carry out operations.

6.6.2. Term

Communications from the Control organism to the NIS will be made immediately, as soon as there is certainty or reasonable indication that the operations analyzed are related to money laundering.

6.6.3 Content

Communications will necessarily contain the following information and documentation:

a) List and identification of the natural or legal persons participating in the operation and the concept of their participation in it.
b) Known activity of the natural or legal persons participating in the operation and correspondence between the activity and the operation.
c) List of related-party transactions and dates to which they refer indicating their nature, currency in which they are carried out, amount, place or places of execution, purpose and payment or collection instruments used.
d) Steps carried out by the reporting obliged subject to investigate the reported operation.
e) Exposure of the circumstances of all kinds from which the indication or certainty of a relationship with money laundering or terrorist financing can be inferred or that show the lack of economic, professional or business justification for carrying out the operation.
f) Any other relevant data for the prevention of money laundering or the financing of terrorism that are determined by regulation.

6.6.4. Form

For communications, form F19-1 attached to this Manual as Annex 12.1 and the means of communication provided in each case by the NIS will be used.

6.7. Refraining from executing suspicious operations

The law establishes the duty to refrain from executing any operation for which there are indications or certainty that it is related to money laundering or the financing of terrorism.

In the event that the internal control organism decides that an operation is suspicious of evidence of money laundering, it will notify the corresponding employee or department by email so that it refrains from executing the operation.

However, according to the Law, when the aforementioned abstention is not possible or could hinder the prosecution of the beneficiaries of the operation, it may be carried out by making the communication immediately after its execution, indicating the reasons that justified the operation. execution of the operation.

6.8. Duty of confidentiality

Trinity Technologies EOOD and its employees, will not reveal to the client or to third parties that information has been communicated to the Executive Service of the Commission, or that any operation is being examined or may be examined in case it could be related to money laundering or terrorist financing.

The internal control organism will establish procedures and measures in place to ensure that the client or third parties are not disclosed that information has been transmitted to the Executive Service or that any operation is being examined in case it could be linked to money laundering.

Likewise, the identity of employees and managers who have made a communication with signs of being suspicious will be kept confidential.

6.9. Collaboration with the commission for the prevention of money laundering and monetary offenses

Regardless of the individual communication of suspicious transactions contained in the previous section, **Trinity Technologies EOOD** will collaborate with said Commission or its support organism, providing, in accordance with current legal regulations, at all times, the documentation and information that is required in the exercise of its powers, on whether they maintain or have maintained throughout the ten previous years

business relationships with certain natural or legal persons and on the nature of said relationships, keeping professional secrecy.

The Representative before the NIS will be responsible for:

- Receive the requirements.
- Execute the necessary internal investigation actions, to respond to the requirements, always within the indicated deadlines.
- Send the response to the Service, containing the required data.

6.10. Internal complaints channel

The obligation is established to **Trinity Technologies EOOD**, as an obligated subject, to have an internal reporting channel where employees can freely report suspected infringement by the company itself, their colleagues or their superiors. Said internal communication must be able to be carried out anonymously.

First, **Trinity Technologies EOOD** makes available to all its employees a postal address and an email of the service provider authorized for this purpose to report any type of incident in which the employee suspects that his immediate supervisor, manager or Internal Control may be related. This telephone is not exclusive for matters regarding the Prevention of Money Laundering and Terrorism Financing, as it can also be used for other issues such as harassment, bribery, etc.

The postal address is:

TRINITY TECHNOLOGIES EOOD

COMPLIANCE DEPARTMENT

2V TOPLI DOL STREET, AP 16, SOFIA, BULGARIA - 1680

Additionally, for matters related to the Prevention of Money Laundering and Terrorism Financing, the email box is available admin@crypto-trinity.com in which emails can be sent from any address to ensure the anonymity of the complainant.

For these purposes, only those indicated above will be considered as internal control and compliance bodies.

7. SYSTEMATIC COMMUNICATION OF OPERATIONS

Anti-Money Laundering Measures Act, adopted on 27 March 2018 and the Rules for the application of the AML Act, adopted on 31 December 2018, relative to the systematic communication of operations, provides that the obliged subjects will communicate to the Executive Service of the Commission with the periodicity determined by the operations that are established by regulation.

The Measures Act has established the operations that must be reported to the NIS on a monthly basis.

If there are no operations susceptible to communication, the obliged subjects will communicate this circumstance every six months.

For the moment, **Trinity Technologies EOOD** is not affected by the obligation to systematically report transactions.

8. PRESERVATION OF DOCUMENTS

Trinity Technologies EOOD will keep, during the established period of 10 years, the following documents:

- Copy of the required documents in application of due diligence measures, for a minimum period of ten years from the termination of the business relationship or the execution of the operation.
- Original or copy of the documents or records that adequately certify the operations, the intervening parties for a minimum period of ten years from the termination of the business relationship or the execution of the operation.
- Reports filed with the authorities on a client's suspicious activity related to a possible money laundering case, along with supporting documentation.
- The records of all courses on the prevention of money laundering taught.
- Any other documents that need to be kept under applicable laws against money laundering.

The aforementioned documentation or information will be properly archived in such a way as to facilitate its location and guarantee its confidentiality.

9. REPRESENTATIVE BEFORE THE NIS AND INTERNAL CONTROL BODY

9.1. The Representative for the NIS

9.1.1. Designation

In the case of legal persons:

In compliance with the provisions of the regulations, a Representative has been appointed to the Executive Service who will act as coordinator of all activities related to the fight against money laundering.

In the case of natural persons:

The representative before the NIS is the owner of the activity.

A substitute has been appointed for cases of prolonged absence, for any reason.

Acts as Representative before NIS Mr. Nikolay Strahilov Gotsev, Passport number: 388751342.

The person of the representative was duly notified to NIS in accordance with Annex 12.2.

9.1.2 Functions

The representative will be responsible for:

- Appear in any administrative or judicial proceedings related to these matters.
- Make communications to NIS regarding operations in which there is certainty or indications of money laundering or financing of terrorism.
- Call meetings of the Internal Control organism.
- Keeping staff promptly informed of any circumstance that could alter the money laundering prevention policy.
- Channel communications addressed to NIS
- Participate in the meetings called by the NIS for consultative or informative purposes.
- Keeping the management body constantly informed of any circumstance that could or should alter or modify the policy for the prevention of money laundering that is carried out.

9.2. The Internal Control Organism

The law establishes that the obligated subjects shall establish an adequate internal control Organism responsible for the application of policies and procedures regarding due diligence, information, document preservation, internal control, evaluation and risk management. , guarantee of compliance with the pertinent provisions and communication, in order to prevent and prevent operations related to money laundering or terrorist financing.

9.2.1. Features

The functions of the Control Organism will be the following:

- Establish policies, procedures, controls and internal regulations for action regarding the prevention of money laundering.
- Prepare and keep the Manual permanently updated, leaving a written record of the modifications, the date of approval and the entry into force.
- Disseminate the necessary information and documentation on prevention among staff.
- Estimate which risk profiles are occurring and which have a greater probability of risk of carrying out money laundering, in order to reinforce the existing money laundering prevention procedures.
- Approve exceptional communication clients.
- Detect, analyze and communicate, where appropriate, to NIS, with criteria of security, speed, efficiency and coordination, all those risky, abnormal, unusual operations in which there are indications or certainty of being related to money laundering.
- Define and implement alerts for the detection of suspicious operations.
- Examine with special attention any transaction that, due to its amount or nature, may be particularly related to money laundering or terrorist financing.
- Receive the communications of operations carried out by the personnel in which there are indications or certainty of being related to the events described above and proceed to their study and assessment.
- Preserve with the utmost diligence the documentation generated by each incident that is reported.

- Decide on the relevance of the communications to be made to the NIS regarding operations in which there are indications or certainty that it is related to money laundering.
- Design and execute training plans for personnel on matters of Money Laundering Prevention.
- Provide NIS and the rest of the authorities (judicial, police, administrative) with the information they require in the exercise of their powers, keeping professional secrecy.
- Periodically analyze the efficiency and effectiveness of the procedures implemented to detect suspicious transactions.
- Manage and control all files generated by mandatory and voluntary communications and requirements.

9.2.2. Faculties

To exercise the above functions, the Internal Control Organism has the following powers:

- Hold urgent or periodic meetings, as appropriate, to examine the communications received from employees or managers, and to fulfill their duties.
- Require the action and collaboration of any employee or organizational unit.
- Request from internal departments, or employees, the documents or files necessary for the investigation of suspicious operations.
- Request information from Public Registries or order commercial reports.
- Request internal departments or employees to implement controls or mechanisms to prevent money laundering.
- Adopt precautionary measures or, where appropriate, decisions about clients.
- Require Internal Audit to verify compliance with the implemented control mechanisms.

The internal control Organism, which will have, where appropriate, representation of the different business areas of the obliged subject, will meet, drawing up express minutes of the resolutions adopted, with the periodicity determined in the internal control procedure.

9.2.3. Composition

The Internal Control and Communication Organism is made up of the following people:

- Nikolay Strahilov Gotsev (Director).
- Cesar Julian Mendez Correa (Director).

9.2.4. Functioning

The Internal Control Organism will meet whenever the circumstances demand and, at least, on a quarterly basis.

Ordinary sessions of the internal control organism will be called by email by the Representative before the NIS, at least 1 calendar week in advance of the scheduled date of the session.

The summons must include at least the date, time, place planned for the meeting and the matters that will make up the Agenda.

The internal control body will be validly constituted when more than half of its components attend. There is no representation. The agreements will be adopted with more than half of the votes in favor.

The agreements of each of its meetings will be collected in the corresponding minutes according to the model of minutes attached to this manual as Annex 12.5, which will form part of the documentation of the money laundering prevention system, and will describe in the reference period:

- The order of the day of the call.
- The matters that have been studied and the agreements adopted
- A summary of the analysis made of the suspicious operations and of the communications made to NIS, if applicable.

The Minutes of the session will be drawn up by the Representative before the NIS, who will forward it to the rest of the members for reading and signing.

9.3. The technical unit for information processing

The Regulation establishes that obligated subjects, whose annual business volume exceeds 50 million euros or whose annual balance sheet exceeds 43 million euros, will have a technical unit for the treatment and

analysis of the information, which must have specialized personnel, in exclusive dedication and with adequate training in analysis.

Trinity Technologies EOOD It is among the assumptions contemplated in the Regulation not to constitute the technical unit, since it does not meet the requirements indicated above

10. STAFF TRAINING

The continuous training of personnel is the basis for the effectiveness of the policy to prevent money laundering and financing of terrorism. Thus, **Trinity Technologies EOOD** establishes as a priority objective the adoption of the necessary measures so that all personnel are aware of the requirements derived from the regulations on the prevention of money laundering.

For this, the internal control organism will organize annual training plans and special courses that, aimed at its managers and employees and specifically at the personnel who perform those jobs that, due to their characteristics, are suitable for detecting events or operations that may be related to money laundering or terrorist financing, train these employees to carry out the detection and know how to proceed in such cases.

These courses may be face-to-face or taught remotely (online training).

The training programs will take into account international standards and national legislation against money laundering and terrorist financing, the latest trends in these criminal activities, as well as the rules and procedures of **Trinity Technologies EOOD** aimed at combating money laundering and terrorist financing, including how to recognize and report suspicious activity.

A record will be kept of all the training actions given, expressly stating its content, if it is carried out in person or remotely, date, duration, name of attendees, percentage of total employees, profile of trainers, as well as a system for evaluating the knowledge acquired.

11. EXAMINATION OF THE BLEACHING PREVENTION SYSTEM

On external examination, establishes that the internal control measures of the obliged subject will be subject to annual examination by an external expert.

The results of the examination will be consigned in a written report that will describe in detail the existing internal control measures, will assess their operational effectiveness and will propose, where appropriate, possible rectifications or improvements. However, in the two years following the issuance of the report, it may be replaced by a follow-up report issued by the external expert, referring exclusively to the adequacy of the measures adopted by the obliged subject to solve the deficiencies identified.

The report will be submitted within a maximum period of three months from the date of issue to the Board of Directors or, where appropriate, to the administrative body or the main governing body of the obligated subject, which will adopt the necessary measures to solve the deficiencies identified.

Nikolay Strahilov Gotsev, Director

12. ANNEXES

12.1. ANNEX I: SUSPICIOUS TRANSACTIONS REPORT

Suspicious Transaction Report (F19-1)

Art. 18 Law 10/2010

Obligated person	
Identification Number	
Representative's name	
Reference of Communication	
Communication Date	

Identification of the people involved

_____

Knowledge of those involved in operations

_____

Description of the operations

_____

Signs of money laundering

_____

Procedures and checks carried out

_____

Documentation submitted

_____

Representative's signature.

12.2. ANNEX II: COMMUNICATION OF PERSON AUTHORIZED BY THE REPRESENTATIVE BEFORE THE NIS

Executive Service of the
Commission of
Prevention of Money
Laundering
and Monetary Offenses

AUTHORIZED PERSON COMMUNICATION (F22-6)

The person who appears in "data of the representative", in his capacity as representative before the Executive Service of the obliged subject mentioned in "data of the obliged subject" authorizes the person whose data are detailed in "data of the authorized person", to sign on his behalf any writing or communication to the Executive Service that he must address in his capacity as representative.

Data of the obliged subject

Type of identification document[10]	Identification document number
Name / Company name	
Surname 1[11]	Surname 2
Type of obligated subject[12]	

Representative details

Type of identification document	Identification document number

[10] ID, Passport, etc.
[11] To be completed exclusively if the obliged subject is a natural person.
[12] It must be selected from the types included in the law.

Name / Company name	
Surname 1	Surname 2
Administration or management position held	
Authorized person data	

Type of identification document	Identification document number

Name	
Surname 1	Surname 2
Home[13]	
Country	Province
Municipality	Postal Code
Telephone	
Email	
Position	

In	,	on

Signature of representative:	Signature of the authorized person:

[13] Address of the work center of the authorized person.

For each person authorized or empowered and for each obligated subject, with a maximum of two people per entity, the following documentation must be sent:

1. Form F22-6 duly completed and signed by both the representative and the authorized person.

2. Document that sufficiently certifies the signature of the authorized person (for example, a copy of the National Identity Document).

All documentation will be sent on paper to the address:

Bulgaria's National Investigation Service (NIS)
Bulevard Doctor G. M. Dimitrov 42, NPZ Dianabad, Sofia, Bulgaria, 1797
Tel. +359 2 982 6666
Web: www.nsls.justice.bg

This authorization extends exclusively to the scope indicated in the first paragraph of the previous page and has an indefinite duration. Its revocation or termination for any reason will be immediately communicated to the Executive Service by means of a written paper signed by the representative, taking effect from the receipt of the communication by said Body.

12.3. ANNEX III: IDENTIFICATION OF CLIENTS AND BENEFICIARIES

12.3.1. Formal identification card of the client: Physical Person

Name / company name: Trinity Technologies EOOD

Register Number: UIC207095476

Address: 2v Topli dol St, ap 16, Sofia, Bulgaria

CP: 1680

CUSTOMER IDENTIFICATION FORM NATURAL PERSON

Date: ....., of ....., 202X

CUSTOMER INFORMATION

Name ..... ID .....

Address ..... ZIP ..... CITY .....

Contact telephone ..... E-mail.....

Business or professional activity .....

Date of commencement of the relationship: ..... of ..... of 202X

Are you a Public Responsibility Person (PRP) ..... if so, indicate what position you hold / have held as PRP .....

Is Relative or Relative of PRP ..... if so, explain what is the relationship of Relative or Relative ....

Documentation attached

A) IDENTIFICATION

Natural persons of Bulgarian nationality:

- The National Identity Document.

Natural persons of foreign nationality:

- The Residence Card.
- The Foreigner Identity Card.
- The Passport or, in the case of citizens of the European Union or the European Economic Area, the document, letter or official personal identity card issued by the authorities of origin.
- The identity document issued by the Ministry of Foreign Affairs and Cooperation for the personnel of the diplomatic and consular representations of third countries in Bulgaria will also be a valid document for the identification of foreigners.

Exceptionally, other personal identity documents issued by a government authority may be accepted as long as they enjoy adequate guarantees of authenticity and include a photograph of the holder.

Identification documents have been verified to be valid.

B) INFORMATION ABOUT YOUR ACTIVITY

One of the following documents will be provided.

- VAT returns (monthly or quarterly, and the annual summary statement).
- Personal income tax return.
- Payrolls of workers for the last month.
- Payment receipts for the self-employed Social Security regime.

12.3.2. Formal identification card of the client: Legal Person

Name / company name: Trinity Technologies EOOD

Register Number: UIC207095476

Address: 2v Topli dol St, ap 16, Sofia, Bulgaria

CP: 1680

CUSTOMER IDENTIFICATION FORM LEGAL PERSON

Date: ....., / ....., /... .....

CUSTOMER INFORMATION

Business name. ..... ID .....

Address ..... ZIP ..... CITY .....

Contact telephone ..... E-mail.....

Business or professional activity .....

Date of commencement of the relationship: ...../..... / .....

REPRESENTATIVE:

Name ..... ID .....

Address ..... ZIP ..... CITY ....

Contact telephone ..... E-mail.....

SHAREHOLDER OR CONTROL STRUCTURE

Name and surname .....ID .....% participation.....

Documentation attached

A) OF IDENTIFICATION.

(The validity of the data consigned in the documentation provided must be accredited by means of a responsible statement from the client. See model 6)

- Public deed of incorporation that contains its company name, legal form, address, the identity of its administrators, statutes and tax identification number.

(In the case of legal persons of Bulgarian nationality, it will be admissible, for the purposes of formal identification, certification from the provincial Mercantile Registry, provided by the client or obtained through telematic consultation).

- Deeds of empowerment of the people who act on their behalf, as well as their identification documents.

- Regarding its shareholding or control structure of the entity, the following is attached:

- **a)** .....
- **b)** .....

In case of legal or voluntary representation:

- Deeds of empowerment of the people acting on their behalf, as well as identification documents of the representative and the person or entity represented.

(It will be admissible the verification by certification of the provincial Mercantile Registry, provided by the client, or obtained through telematic consultation)

In entities without legal personality:

- They carry out business activity:

Proof of identity documents are provided for all participants.

- They do not carry out business activity:

Identification document of the person acting on behalf of the entity is provided.

B) RELATING TO ITS ACTIVITY

One of the following documents will be provided.

- VAT returns (monthly or quarterly, and the annual summary statement).
- Corporate Tax Declaration.
- Annual accounts presented in the Mercantile Registry.
- Payrolls of workers for the last month.
- Other documentation:

12.3.3. Responsible Declaration

Name / company name .....

ID ..... Address: .....

Postcode / City.....

ADDRESS:

Name / company name: Trinity Technologies EOOD

Register Number: UIC207095476

Address: 2v Topli dol St, ap 16, Sofia, Bulgaria

CP: 1680

RESPONSIBLE DECLARATION ON IDENTIFICATION DOCUMENTS

In application of the law, which approves the Regulation on the prevention of money laundering and terrorist financing,

....., as legal representative / administrator of ..... EOOD, according to powers that appear in public deeds dated ..... / .... / ..... and notary ....., declares that the documents delivered to the obligated subject are current.

RESPONSIBLE DECLARATION ON PROPERTY / PRP IN LEGAL PERSONS

In application of the Law, on the prevention of money laundering and terrorist financing, ..., as legal representative / administrator of ..... EOOD, according to powers that appear in a public deed dated ..... / .... / ..... and notary ....., certifies the following (options to choose from):

1. That the following people and entities are registered in the entity's membership book, and their degree of participation:

- .....
- .....
- .....

(List of individuals who ultimately own or control, directly or indirectly, a percentage greater than 25% of the capital or voting rights of the entity, or who by other means exercise direct or indirect control of management. A copy of the necessary documents must also be provided; such as partner books or public deeds)

2. That in the absence of natural persons who own or control, directly or indirectly, a percentage greater than 25% of the capital or voting rights of the entity, in application of the Regulations, it is considered that the entity exercises control. administrator / s of the entity, whose identification data / s are listed below:

- Name / company name: ..... Register Number ....

In the event that there is a “real owner” of the entity, please indicate if any of these is a Public Responsibility Person (“PRP”), or a Family member or relative of the same.

- Yes
- No

Indicate name and surname and what is the position of PRP: .....

Explain what is the relationship of Relative or Relative: .....

By means of this certification, the undersigned is responsible for the veracity of the data provided, for the purposes of compliance with the obligations established by the Law, and its development regulations, by the obliged subject.

In ....., on ..... / ..../ .....

Signed. As .....

12.4. ANNEX V: OCIC MODEL OF MINUTES MEETING

MINUTES OF THE MEETING OF THE INTERNAL CONTROL AND COMMUNICATION BODY OF TRINITY TECHNOLOGIES EOOD, HELD ON ...../ ..... /.....

In Sofia, on ..... / ...../....., at the registered office 2v Topli dol St, ap 16 - 1680, all the components of the company's internal control and communication body, unanimously agreed to constitute a session of this body.

ASSISTANTS:

NAME POSITION

.....

.....

.....

.....

.....

.....

.....

.....

.....

All attendees sign the previous list of attendees by rubric in the margin of their respective names.

ORDER OF THE DAY:

As items on the Agenda, the following were unanimously agreed:

1. Analysis and examination of the operations carried out in the previous xxxxxx months, insofar as it could have any relevance with the regulations on the prevention of money laundering and terrorist financing.
2. Activity in the system.
3. Agreements adopted.
4. Reading and approval of the minutes of the session.

OPENING OF THE SESSION:

Once the session was opened, the representative before the NIS took the floor, who went on to report on the need to analyze and examine whether during the xxxxx months prior to the date of this meeting, there has been any operation in the activity of the company that in any way could be relevant in terms of regulations on the prevention of money laundering and terrorist financing.

The member of the Control Body responsible for the analysis of operations, reported that:

(SUMMARY OF THE ANALYSIS AND THE COMMUNICATIONS MADE TO THE NIS)

Regarding the activity taking place in the system, the representative before the NIS reported that in the course of the past months, the following issues stand out:

(OUTSTANDING FACTS IN THE PREVENTION SYSTEM)

Likewise, and in relation to the proper functioning of the prevention system, the following agreements were adopted:

(AGREEMENTS ADOPTED IN REALIZATION WITH THE PREVENTION SYSTEM)

APPROVAL OF THE MINUTES:

Subsequently, the session was suspended for a brief moment, in order to draw up these minutes, which were subsequently read by the person in charge before the NIS and approved unanimously and without any opposition.

(SIGNATURE OF THE MEMBERS OF THE CONTROL BODY)

12.5. ANNEX VI: RISK OPERATIONS CATALOG

EXEMPLIFICATION CATALOG OF MONEY LAUNDERING RISK OPERATIONS IN THE ACTIVITIES OF TRINITY TECHNOLOGIES EOOD

A. Characteristics of the participants

A.1 Natural persons:

a. Operations involving people domiciled in tax havens or risk territories, when the means of payment used by them meets any of the characteristics of those included among the risk operations, detailed in this document.
b. Operations that are carried out on behalf of minors, people over 70 years of age or who show signs of mental disability or with obvious indications of lack of economic capacity for such acquisitions.
c. Operations involving people who occupy or have occupied prominent political positions, high positions or similar in generally non-democratic countries, including their close family environment.
d. Operations involving people who are prosecuted or convicted of crimes or turn out to be public or notorious for their alleged relationship to criminal activities is suspected, provided that they allow illicit enrichment and that they can be considered as underlying the crime of money laundering., as well as those made by people related to the above (e.g by family ties, professionals, of origin, in which there is a coincidence in the address or coincidence of representatives or attorneys, etc.).
e. Operations involving people with an unknown address or mere correspondence (e.g PO box, shared offices, professional offices, etc.), or with supposedly false or probable uncertainty data.

g. Several operations in which the same participant participates. As well as those carried out by groups of people who may be related to each other (eg by family ties, by professional ties, by people of the same nationality, by people in whom there is a coincidence in the domicile or coincidence of representatives or attorneys-in-fact, etc).

A.2 Legal persons:

a. Operations involving legal persons domiciled in tax havens or risk territories, when the means of payment used by them meets any of the characteristics of those included among the risk operations detailed in this document.
b. Operations involving recently established legal persons when the amount is high in relation to their assets.
c. Operations in which legal persons intervene when it does not appear that there is a relationship between the characteristics of the operation and the activity carried out by the purchasing company or it does not carry out any activity.
d. Operations involving legal persons whose owners occupy or have occupied prominent political positions, high positions or similar in generally non-democratic countries, including their close family environment.
e. Operations involving Foundations, Cultural and Recreational Associations and, in general, non-profit entities, when the characteristics of the operation do not correspond to the objectives of the entity.
f. Operations involving legal persons, which, even though they are registered in Bulgaria, are constituted mainly by foreign citizens or non-residents in Bulgaria.
g. Operations involving legal persons with an unknown address or mere correspondence (e.g PO box, shared offices, professional offices), or with supposedly false or probable uncertainty data.
h. Several operations in which the same participant participates. As well as those carried out by groups of legal persons that may be related to each other (for example, by family ties of their owners or proxies, by professional ties of the same, by coincidence in the nationality of either the legal persons or of their owners or proxies, by coincidence in the domicile of the legal persons or their owners or

proxies, by coincidence of the owner, representatives or proxies, by the similarity of names of legal persons, etc.).

i. Operations involving legal persons in which the only known activity is investment in real estate as a mere possession thereof.

A.3 Behavior of the parties involved, either a natural or legal person:

a. Operations in which there are indications or certainty that the parties are not acting on their own, trying to hide the identity of the real client.
b. Operations in which the parties are not residents of Bulgaria:

B. Characteristics of the operation:

- Disposal in cash in short periods of time for different operations linked to each other that exceed 1,000 euros or that in longer periods exceed 10,000 euros.
- Cash withdrawals for high or maximum amounts (€300) in short periods of time to the same people or telephone numbers that exceed the amount of 1,000 euros.
- Operations or cash withdrawals in short periods of time to persons other than the issuer or telephone numbers other than the issuer that exceed amounts of 2,500.
- Unrelated operations carried out by the issuer on the same telephone number that exceed the amount of 10,000 euros.
- Operations not linked to each other but carried out to a person other than the issuer or a different telephone number that exceed amounts greater than 15,000 euros.
- Operations that exceed the maximum thresholds for buying or selling cryptocurrencies established by **Trinity Technologies EOOD**.
- Cash payments in which one of the intervening parties acts as an entrepreneur or professional for amounts greater than 2,500 euros in accordance with the law.

- Money laundering from criminal activities such as scams carried out on citizens through identity theft, the **Trinity Technologies EOOD** platform being the means to obtain the scammed money laundering.

a. By Typology
b. By the Interveners
c. For the amount of the operations.

Examples of suspicious transactions:

A. When the nature or volume of the client`s active or passive operations does not correspond to their activity or operational history.
B. When the same account, without justifying cause, has been paid through cash income by a large number of people or receives multiple cash income from the same person.
C. Plurality of transfers made by several originators to the same beneficiary abroad or by a single originator abroad to several beneficiaries in Bulgaria, with no business relationship being appreciated between the parties.
D. Movements with origin or destination in territories or countries at risk.
E. Transfers that do not contain the identity of the originator or the number of the account that originated the transfer.
F. Operations with agents that, due to their nature, volume, amount, geographical area or other characteristics of the operations, differ significantly from the usual or ordinary of the sector or from those of the obliged subject.
G. The types of operations established by the Commission. These operations will be published or communicated to the obligated subjects, directly or through their professional associations. Some examples:

- Anonymous clients.
- Impossibility of knowing or verifying customer data.
- Clients who refuse or resist providing the information necessary to know their activities or the normal information in a professional relationship.

- Clients who provide false or erroneous information or information that is difficult to verify.
- Clients residing in tax havens, in countries or territories not cooperating in the fight against money laundering and terrorist financing, or in States where there is knowledge of the existence of particularly active criminal organizations (for example, drug trafficking, activities terrorists, organized crime or human trafficking).
- Clients with published police or criminal records, or linked to persons subject to a ban on operating or terrorist financing activities.
- Clients who have the condition or are related to 'people from the political'.
- Clients who provide the same address or telephone number as another client, with whom they do not appear to have a relationship.
- Clients who end the professional relationship when requested to provide information.
- Clients for whom there are indications that they are acting on behalf of another, trying to hide the identity of the real client.
- Operations in which unusual or unnecessarily complex legal figures are used that apparently lack economic logic.
- Operations that do not correspond to the nature, volume of activity or operational history of the client.
- Operations in which the payment is made through funds from tax havens, countries or territories not cooperating in the fight against money laundering and terrorist financing, or States where there is knowledge of the existence of particularly active criminal organizations (for example, drug trafficking, terrorist activities, organized crime or human trafficking).

12.6. ANNEX VII: TAX HAVENS AND OTHER RISK TERRITORIES

1. LIST OF TAX HAVENS

In accordance with the International Money Funds, will be considered tax havens:

1. Anguilla
2. Antigua and Barbada
3. Bermuda
4. Emirate of the State of Bahrain
5. Fiji
6. Gibraltar
7. Granada
8. Isle of Man
9. Cayman Islands
10. Cook Islands
11. Islands of Guernsey and Jersey (Channel Islands)
12. Falkland Islands
13. Mariana Islands
14. Solomon Islands
15. Turks and Caicos Islands
16. British Virgin Islands
17. Virgin Islands of the United States of America
18. Macau
19. Mauritius
20. Montserrat
21. Principality of Liechtenstein
22. Principality of Monaco

23. Hashemite Kingdom of Jordan
24. Republic of Dominica
25. Republic of Liberia
26. Republic of Nauru
27. Republic of Seychelles
28. Republic of Vanuatu
29. Lebanese Republic
30. Saint Vincent and the Grenadines
31. Saint Lucia
32. Sultanate of Brunei
33. Sultanate of Oman

The aforementioned countries and territories that sign an information exchange agreement with Bulgaria on tax matters or an agreement to avoid double taxation with an information exchange clause will cease to be considered tax havens at the time said agreements or agreements come into force.

Currently, the following countries or territories have been removed from the list of tax havens, for having signed the corresponding information exchange agreements in tax matters or agreements to avoid double taxation with an information exchange clause:

1. Netherlands Antilles
2. Aruba
3. Barbados
4. United Arab Emirates
5. Hong Kong
6. Jamaica
7. The Bahamas
8. Luxembourg
9. Malta
10. Panama
11. Principality of Andorra
12. San Marino
13. Singapore
14. Trinidad and Tobago

LIST OF NON-COOPERATING COUNTRIES

Its an obligation to communicate operations in relation to certain countries to NIS, the following are considered non-cooperating countries:

1. Egypt
2. Philippines
3. Guatemala
4. Indonesia
5. Myanmar (former Burma)
6. Nigeria
7. Islamic Republic of Iran
8. Ukraine
9. Russia
10. Belarus

2. LIST OF HIGH RISK THIRD COUNTRIES WITH STRATEGIC DEFICIENCIES ACCORDING TO THE COMMISSION EUROPEAN

Commission Delegated Regulation (EU) 2016/1675 of July 14, 2016, which completes Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, establishes the list of third country jurisdictions that have strategic deficiencies in their regimes to combat money laundering and terrorist financing and that pose significant threats to the financial system of the European Union.
In accordance with said Delegated Regulation, the following categories and jurisdictions are identified:

Third high-risk countries that have submitted a written commitment at a high political level to remedy identified deficiencies and have developed an action plan with the FATF:

1. Afghanistan
2. Bosnia and Herzegovina
3. Iraq
4. Laos PDR
5. Syria
6. Uganda
7. Vanuatu

8. Yemen

Third high-risk countries that have presented a high-level political commitment to remedy the deficiencies found and have decided to request technical assistance to implement the FATF Action Plan, and that have been identified in a FATF Public Statement:

1. Iran

High-risk third countries that currently present significant risks of money laundering and terrorist financing due to having repeatedly failed to comply with the obligation to correct the deficiencies found, and which have been identified in a FATF Public Statement:

1. Democratic People's Republic of Korea (DPRK)

3. LIST OF HIGH RISK COUNTRIES AND JURISDICTIONS ACCORDING TO THE FATF

Countries with respect to which the FATF has requested its members and other jurisdictions to apply appropriate countermeasures to protect the international financial system from the significant risk they present:

1. North Korea
2. Iran

Countries that present strategic deficiencies in the system implemented to combat ML / TF, having not adopted sufficient measures to face them or not having the commitment to adopt an action plan with the FATF to do so. The FATF requests that its members evaluate the risks that may arise from the deficiencies associated with each of these countries, which are detailed in the aforementioned report:

1. Algeria
2. Myanmar

Countries that present strategic deficiencies in the system implemented to combat ML / TF and have developed an action plan with the FATF to address them, having committed in writing to their compliance by the highest political level:

1. Ethiopia
2. Iraq
3. Serbia
4. Syria
5. Sri Lanka
6. Trinidad and Tobago
7. Tunisia
8. Vanuatu
9. Yemen

4. COUNTRIES, TERRITORIES OR JURISDICTIONS SUBJECT TO SANCTIONS, EMBARGOES OR ANALOGUE MEASURES APPROVED BY THE EUROPEAN UNION, THE UNITED NATIONS OR OTHER INTERNATIONAL ORGANIZATIONS

By virtue of the provisions of Chapter VII of the United Nations Charter, the United Nations Security Council can adopt coercive measures to maintain or restore international peace and security. These measures include financial sanctions or of any other nature.

5. COUNTRIES, TERRITORIES OR JURISDICTIONS THAT PRESENT SIGNIFICANT LEVELS OF CORRUPTION OR OTHER CRIMINAL ACTIVITIES

The International Organization for Transparency International publishes, annually, the Corruption Perception Index. The Corruption Perception Index corresponding to a country or territory indicates the degree of corruption in the public sector according to the perception of businessmen and country analysts, between 100 (perception of the absence of corruption) and 0 (perception of very corrupt).

As an example, Bulgaria has a Corruption Perception.

According to the data contained in the latest publication of the Corruption Perception index (year 2017), the countries with the highest Corruption Perception index were the following:

Iraq (18)
Venezuela (18)
North Korea (17)
Guinea Bissau (17)
Equatorial Guinea (17)
Libya (17)
Sudan (16)
Yemen (16)
Afghanistan (15)
Syria (14)
South Sudan (12)
Somalia (9)

6. COUNTRIES, TERRITORIES OR JURISDICTIONS IN WHICH FINANCING OR SUPPORT TO TERRORIST ACTIVITIES IS FACILITATED

There is currently no objective data regarding the countries, territories or jurisdictions that facilitate the financing or support of terrorist activities.

7. COUNTRIES, TERRITORIES OR JURISDICTIONS PRESENTING A SIGNIFICANT EXTRATERRITORIAL FINANCIAL SECTOR (OFF-SHORE CENTERS)

With a regulatory nature, there is no catalog or list of offshore jurisdictions in Bulgaria. There are different international organizations that have prepared analyzes and lists of these types of territories.

12.7. ANNEX VIII: LISTINGS OF PERSONS AND ENTITIES SUBJECT TO FINANCIAL SANCTIONS IN EUROPE AND THE UNITED STATES

Among the list of sanctions imposed by the United Nations Security Council you can find the link:
https://www.un.org/sc/suborg/es/sanctions/un-sc-consolidated-list

The list of all persons and entities subject to sanctions imposed by the Security Council can be consulted from the following link:
https://scsanctions.un.org/search/

Consolidated list of the European Union

Likewise, within the framework of the Common Foreign and Security Policy, the European Union may apply restrictive measures or sanctions under the provisions of Article 24 of the Treaty on European Union.

Consolidated list of individuals, groups and entities subject to financial sanctions by the European Union:
http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm

Access to the search for people or entities can be done through the following link:
https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions
www.sanctionsmap.eu

12.8. ANNEX IX. RISK SHEET

Name / company name: Trinity Technologies EOOD

Register Number: UIC207095476

Address: 2v Topli dol St, ap 16, Sofia, Bulgaria

CP: 1680

CLIENT'S RISK CARD

Date: ....., / ....., / ... .

(customer identification data)

Name / company name ..... ID .....

Address: ..... CP ..... CITY ....

CUSTOMER IDENTIFICATION

Name / Company name ……../……..

ID:……..

Business or professional activity

Relationship start date On..... / ..... / ....

CLIENT CLASSIFICATION (check the one that applies)

□ NO RISK

□ AVERAGE RISK

□ HIGH RISK

A. Level of seniority of the client.

□ New

□ Habitual. Start date of the relationship .....

B. Geographic, international and national risk.

□ No risk

□ Address, branches or operations in tax haven .....

□ Risk zone in Bulgaria .....

□ Other risks .....

C. Risk of the client's business / economic activity.

□ No risk

□ Client activity considered risky by .....

□ Other situations .....

D. Background of the client, in the case of natural persons.

□ Natural persons who carry out or have carried out public functions

□ Client included in a sanction list of international organizations

E. Other factors:

□ ……..……

12.10. ANNEX X. SUSPECT OPERATIONS REVIEW SHEET

SUSPECT OPERATIONS REVIEW SHEET

PREVENTION OF MONEY LAUNDERING

Name / company name: Trinity Technologies EOOD

Register Number: UIC207095476

Address: 2v Topli dol St, ap 16, Sofia, Bulgaria

CP: 1680

SUSPECT OPERATIONS REVIEW SHEET

CLIENT

Name / Company name ……..

ID ……

Business or professional activity ……..

Relationship start date ……. on ……. / ……. ……

1. EMPLOYEE PERFORMING THE OPERATION REVIEW:

..... Department .....

2. EXAM FINISHED ON DATE .... **on** ..... / .....

3. CHARACTERISTICS OF THE OPERATION. (fill in the appropriate information in each case)

a. List and identification of the natural or legal persons participating in the operation and the concept of their participation in it.
b. Known activity of the natural or legal persons participating in the operation and correspondence between the activity and the operation.
c. Description of the operations: dates, currency in which they are carried out, amount, place or places of execution, purpose and payment or collection instruments used.
d. Steps carried out by the reporting obliged subject to investigate the reported operation.
e. Exposure of the circumstances of all kinds from which the indication or certainty of a relationship with money laundering or terrorist financing can be inferred or that show the lack of economic, professional or business justification for carrying out the operation.
f. Existing documentation.

4. EXAM RESULTS:

- FINALLY, NO SIGNS OF SUSPICIOUS OPERATION ARE APPRECIATED
- REFERRAL TO THE REPRESENTATIVE BEFORE THE NIS

In ....., on ..... / .... / .....

Signed.: ..... (The employee)