Anti-Money Laundering and Know Your Customer Policy

INTERNAL PROCEDURE FOR COUNTERACTING MONEY LAUNDERING AND TERRORIST FINANCING REFERRED TO IN ARTICLE 50 POLISH ACT OF 1 MARCH 2018 ON COUNTERACTING MONEY LAUNDERING AND TERRORIST FINANCING

Walluta Europe Sp. z o.o. with its registered seat in Łódź

116/52 Piotrkowska Street

90-006 Łódź

Republic of Poland

NIP (TIN): 7252327520

REGON (Statistical Number): 524238470

KRS (Commercial Number): 0001014691

Issued and Approved by: President of the Management Board - senior management member responsible for the performance of the obligations resulting from provision of money laundering and terrorist financing regulations according to Article 6 of Polish AML Act

Information on issuance or revisions of AML Policy:

Date	Information	Responsible person
29.12.2023 version 2	Preparation and approval by the Management Board Internal Procedure for Counteracting Money Laundering and Terrorist Financing referred to in Article 50 Polish Act Of 1 March 2018 on Counteracting Money Laundering And Terrorist Financing considering the new quarterly reporting obligation via GIIS starting from 01.01-18.01.2024.	Werner Wildberger
20.01.2023 version 1	Preparation and approval by the Management Board Internal Procedure for Counteracting Money Laundering and Terrorist Financing referred to in Article 50 Polish Act Of 1 March 2018 on Counteracting	Werner Wildberger

	Money Laundering And Terrorist Financing	

Definitions:

Terms used below shall have the following meaning in whole AML Policy and Annexes

a) AML Officer - employee holding a management position, responsible for ensuring the compliance of activity of the obligated institution and its employees and other persons performing activities for the Walluta Europe Sp. z o.o. with the provisions on money laundering and terrorist financing according to Article 8 of Polish AML Act. If AML Officer has not been appointed or is temporarily absent for health or other reasons, the responsibility and functions of the AML Officer bears on the Management Board Member, designated to the area of AML compliance in the Company with accordance with Article 6 and 7 of Polish AML Act;
b) AML Policy – this document, Internal Procedure for Counteracting Money Laundering and Terrorist Financing referred to In Article 50 Polish Act Of 1 March 2018 on Counteracting Money Laundering And Terrorist Financing;
c) AML Specialist – employee, who perform complex assessments of the Customers' documents, which are obtained during the Customers' document verification and after financial security measures make decisions for establishing of business relationships and opening Customers' accounts. In case Company does not employ AML Specialists, his or her duties are performed by AML Officer;
d) Company - Walluta Europe Spółka z ograniczoną odpowiedzialnością with its registered seat in Lodž, Republic of Poland (hereinafter: "Walluta Europe"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS number: 0001014691, held by District Court for the city of Łódź-Śródmieście in Łódź, 20th Commercial Division of National Court Register.
e) Company System – technological solutions, including software and Customer relationship management, which is use to manage interactions with Customers and potential Customers;
f) Customer – natural or legal persons, with whom or with which Company is entering into business relation or occasional transaction;
g) GIIF - the authority of Polish government administration exercising control over the compliance with the provisions on counteracting money laundering and terrorist financing; full name "General Inspector of Financial Information"; Polish name: "Generalny Inspektor Informacji Finansowej"; address: Świętokrzyska 12 Street, 00-916, Łódź, Republic of Poland.
a) Polish AML Act - the Polish Act of 1st March 2018 on counteracting money laundering and financing terrorism (Polish Journal of Laws 2023, item. 1124, 1285, 1723, 1843 - consolidated text);

AML Policy content

1. Walluta Europe Spółka z ograniczoną odpowiedzialnościąwith its registered seat in Lodž, Republic of Poland (hereinafter: "Walluta Europe"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS number: 0001014691.
2. The issue of anti-money laundering and counteracting terrorism has been regulated in:
   b) the Polish Act of 1st March 2018 on counteracting money laundering and financing terrorism (Polish Journal of Laws 2023, item. 1124, 1285, 1723, 1843 - consolidated text);
   c) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73)
   d) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (*OJ L 156, 19.6.2018, p. 43–74)*
3. Money laundering shall be understood as the act referred to in Article 299 of the Act of 6 June 1997 – Polish Penal Code, that is:

   Art. 299

   § 1. Anyone who receives, transfers or transports abroad, or assists in the transfer of title or possession of legal tender, securities or other foreign currency values, property rights or real or movable property obtained from the profits of offences committed by other people, or takes any other action that may prevent or significantly hinder the determination of their criminal origin or place of location, their detection or forfeiture, is liable to imprisonment for between six months and eight years.

   § 2. Anyone who, as an employee of a bank, financial or credit institution, or any other entity legally obliged to register transactions and the people performing them, unlawfully receives a cash amount of money or foreign currency, or who transfers or converts it, or receives it under other circumstances raising a justified suspicion as to its origin from the offences specified in § 1, or who provides services aimed at concealing its criminal origin or in securing it against forfeiture, is liable to the penalty specified in § 1.
4. Terrorist financing shall be understood as the act referred to in Article 165a of the Act of 6 June 1997 – Polish Penal Code; that is:

   Art. 165a

   Anyone who collects, transfers or offers means of payment, financial instruments, securities, foreign exchange, property rights or other movable or immovable property in order to finance a terrorist offence is liable to imprisonment for between two and 12 years.
5. The aim of money laundering is to transfer the proceeds from criminal activity into a legitimate financial space and business cycle. Detailed criteria as to when money laundering is considered such in a legal sense are specified in the Law.
6. The process of money laundering can be divided into three stages: placement, layering, and integration:
   a. Placement

Introduction of cash or other physical valuables originating from illegal / criminal activities into financial or non-financial institutions.

b. Layering
Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

c. Integration
Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

7. Financial/non-financial institutions may be misused at any point in the money laundering process.
8. Money laundering shall be regarded as such regardless of whether the exact criminal act from which funds are derived has been identified.
9. Financing of terrorism is collection or transfer of any funds or other assets, whether directly or indirectly, to be used for (or with knowledge that they will be used for, either in full or in part) committing acts of terror or any related action.
10. The financing of the manufacture, storage, transfer, use or distribution of weapons of mass destruction (hereinafter referred to as proliferation) – any direct or indirect collection or transfer of funds or other property obtained in any form, with a view to using them or knowing that they will be used in whole or in part to finance proliferation.
11. Virtual currencies are developing quickly and are an example of digital innovation. However, at the same time, there is a risk that virtual currencies could be used by terrorist organizations to circumvent the traditional financial system and conceal financial transactions as these can be carried out in an anonymous manner.
12. Walluta Europe performs business activity consisting in the provision of services in the scope of providing virtual assets services. According to Polish AML Act, scope of the business activity of Walluta Europe has to be recognized as exchange between virtual currencies and means of payment. According to Article 2 point 1 section 12 letter a of Polish AML Act Global Trade Research has to be recognized as “obligated entity”.
13. The authority of Polish government administration exercising control over the compliance with the provisions on counteracting money laundering and terrorist financing is the General Inspector of Financial Information, hereinafter referred to as the “GIIF”, Świętokrzyska 12 Street, 00-916, Łódź, Republic of Poland.
14. This Policy outlines the minimum general unified standards of internal KYC / AML control which would be adhered to by Walluta Europe in order to mitigate the legal, regulatory, reputational, operational, and as a consequence financial risks.
15. The main objectives of this policy are:
    a) prevent Walluta Europe from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities;
    b) enable Walluta Europe to know and understand its Customers with which Walluta Europe has any financial dealings with and their financial background and source of funds better, which in turn would help it to manage its risks prudently;

c) compliance with all applicable regulations, rules and laws and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in Walluta Europe business;
a) put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, procedures and regulatory guidelines; and
b) equip Walluta Europe`s personnel with the necessary training and measures to deal with matters concerning KYC/AML procedures and reporting obligations.

16. This Policy and defined KYC and AML procedures are revisited periodically and amended from time to time (especially in relation to changes in the risk factors concerning Customers, countries or geographical areas, products, services, transactions or their delivery channels – according to art. 27 point 3 Polish Act of 1st March 2018 on counteracting money laundering and financing terrorism) based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing.
17. This Policy is subject to approval by the senior management of Walluta Europe.

Customer identification – KYC Procedure

18. In order to establish business relation with Walluta Europe, Customers have to proceed through specific identity verification procedure.
19. The aim of this section is to ensure the proper identification and verification of Customers participating in transactions, as well as ongoing monitoring of business relationships, including transactions carried out during business relationships, regular verification of data used for identification, update of relevant documents, data or information and, when necessary, identification of the source and origin of funds used in transactions.
20. Customer due diligence is one of the main tools for ensuring the implementation of legislation aimed at preventing money laundering and terrorist financing and at applying sound business practices.
21. Customer due diligence comprises a set of activities and practices arising from the organizational and functional structure of Walluta Europe and described in internal procedures, which have been approved by the directing bodies of the Walluta Europe and the implementation of which is subject to control systems established and applied by internal control rules.
22. The purpose of Customer due diligence is to prevent the use of assets and property obtained in a criminal manner in the economic activities of credit institutions and financial institutions and in the services provided by them whose goal is to prevent the exploitation of the financial system and economic space of the Republic of Poland for money laundering and terrorist financing. Customer due diligence is aimed, first and foremost, at applying the Know-Your-Customer principle, under which a Customer shall be identified and the appropriateness of transactions shall be assessed based on the Customer's principal business and prior pattern of payments. In addition, Customer due diligence serves to identify unusual circumstances in the operations of a Customer or circumstances whereby an employee of Walluta Europe has reason to suspect money laundering or terrorist financing.
23. Customer due diligence ensures the application of adequate risk management measures in order to ensure constant monitoring of Customers and their transactions and the gathering and analysis of relevant information. Upon applying the Customer due diligence measures, Walluta Europe will follow the principles compatible with its business strategy and, based on prior risk analysis and depending on the nature of the Customer's business relationships, apply Customer due diligence to a different extent.

24. Customer due diligence are applied based on risk sensitive basis, i.e. the nature of the business relationship or transaction and the risks arising therefrom shall be taken into account upon selection and application of the measures. Risk-based Customer due diligence calls for the prior weighing of the specific business relationships or transaction risks and, as a result thereof, qualification of the business relationship in order to decide on the nature of the measure to be taken (for instance, normal, enhanced or simplified due diligence measures could be applied).
25. Upon establishing a business relationship, Walluta Europe will identify the person and verify their right of representation based on reliable sources, identify the beneficial owner and, in the case of companies, the control structure, as well as identify the nature and purpose of possible transactions, including, if necessary, the source and origin of the funds involved in the transactions.
26. Customer due diligence measures are appropriate and with suitable scope if they make it possible to identify transactions aimed at money laundering and terrorist financing and identify suspicious and unusual transactions as well as transactions that do not have a reasonable financial purpose or if they at least contribute to the attainment of these goals.
27. Where the risk associated with a business relationship is low, and to the extent permitted by national legislation, Walluta Europe applies simplified Customer due diligence measures (SDD). Where the risk associated with a business relationship is increased, Walluta Europe applies enhanced Customer due diligence measures (EDD).

Natural person Customer identification

28. To enter into business relation with Walluta Europe Customer who is natural person has to provide following data:
    a. Full Name (with first name and last name separation);
    b. Residential Address;
    c. Citizenship;
    d. Number entered in the Polish Universal Electronic System for Civil Registration (PESEL)-if applicable or date of birth and place of birth in the case if the PESEL number has not been signed;
    e. Series and number of the document confirming the identity;
    f. residence address
    g. The name (business name), the tax identification number (TIN - pl: ”NIP”) and the address of the main place of business activity - in the case of a natural person conducting business activity.
29. Customers should submit their identification data and other information (address verification document, information about payment methods) requested by Walluta Europe, doing registration process in the Walluta Europe system, or provide such data to the AML Specialist after AML Specialist request.
30. Verification of identity is required by obtaining a high-resolution, non-expired copy of the Customer’s government-issued ID:
    a. internal passport or International Passport (two pages), the photocopy of the passport shall be dated and signed by the natural person, with the indication “for Walluta Europe Sp. z o.o.”;
    b. ID card only with MRZ code (both sides), the photocopy of the ID card shall be dated and signed by the natural person, with the indication “for Walluta Europe Sp. z o.o.”;
    c. driving license - if the name, photograph or facial image, s, date of birth, citizenship or personal identification code of the holder are entered therein.

31. Natural person should submit a national identity document issued by the resident country, or equivalent identity document, or identity document, which is valid for entry into the country there identification are taken.
32. Walluta Europe verifies the correctness of the data specified in this section, using information originating from a credible and independent source for that purpose.
33. The AML Specialist using the personal identity verification and document verification systems provided by Tangany GmbH shall perform the following checks:
    a. Face Match Check, which allow to confirm matches of an image of a person face among a range of other photo images found in various documents, for example a passport, on name badge, a driver's license or other photo ID as well as selfies or avatar images. A completed search results in a "match" or "doesn't match" result. Required data for input: image of person face and images of document containing the image of the persons face;
    b. Identity Check, which allow to verify of a person identity by matching persons data against data from multiple document check databases that cover at least 190+ countries and over 11 000 sample types of government-issued ID documents.
34. After providing of necessary information the Walluta Europe's third party KYC/KYB and AML screening provider Tangany GmbH makes checks in diverse screening databases, including data present in UN Sanctions Map and Global Watchlist.
35. The database of a variety of lists across the globe that the partner uses to run regular identity checks against known or suspected terrorists, money launderers, frauds or PEPs. The watchlist includes domestic and international, government, law enforcement and regulatory databases that store information on individuals who are on a criminal list or prohibited in certain industries such as finance and healthcare. Among such people are specially designated nationals, terrorists, narcotics traffickers, money launderers, blocked persons, parties subject to various economic sanctioned programs who are forbidden from conducting business and those involved in the proliferation of mass destruction weapons.).
36. If the Customer wants to continue collaboration with Walluta Europe he/she should to pass full verification process and provide requested documents.
37. The potential or existing Customer shall present identity (personal) documents to Walluta Europe:
    a. in the form of original document (natural and legal entities) for identification in person;
    b. in the form of uncertified copies for remote identification.
38. The Customer's identity (personal) document and other documents submitted to Walluta Europe shall satisfy the following requirements:
    a. Identity documents of natural entities shall contain the information listed in clause 28;
    b. The documents shall be valid (the validity term specified in the document has not expired at the time of presentation to Walluta Europe, and the document is not declared invalid);
    c. The documents should contain no evident signs of falsification, corrections, cross-outs or deletions;
    d. The documents should contain no damages (water, stains of dye, punches, etc.);
39. Verification of residence is required by obtaining a copy of an acceptable address proof document issued in the 3 months prior to establishing an business relationship with Walluta Europe. The document must carry the Customer's name and address. A valid proof of residence document can be:
    a. bank statement;
    b. debit or credit card statement;

c. utility bill (water, electricity, gas, internet, phone);
d. payroll statement or official salary document from employer;
e. insurance statement;
f. tax document; or
g. residence certificate.

Business entity Customer identification

40. To enter into business relation with Walluta Europe Customer who is a legal person or an organizational unit having no legal personality to whom legal capacity is granted under an act has to provide following data:

    a. the name (business name);
    b. the organizational form;
    c. the address of the registered office or the address of conducting business;
    d. the Tax Identification Number (pl: ”NIP”);
    e. commercial registration number;
    f. date of registration;
    g. the identification data and measures stipulated in point 12, 13, 14, 15 of the natural person representing entity.

41. Walluta Europe verifies the legal status of the legal entity through proper and relevant documents, in particular:

    a. Excerpt from Commercial Register;
    b. Founding act of legal entity;
    c. A legal document relating to the formation of a company or corporation (Certificate of Incorporation/Registration/Formation). It is a license to form a corporation issued by the government or, in some jurisdictions, by non-governmental entity/corporation;
    d. The memorandum of association (Memorandum & Articles of Association/By Laws/Partnership Agreement), which is the document that sets up the company and the articles of association set out how the company is run, governed and owned. The articles of association will therefore include the responsibilities and powers of the directors and the means by which the members exert control over the Member of the Board;
    e. A share certificate (Shareholder certificate and register), which is a written document signed on behalf of a corporation that serves as legal proof of ownership of the number of shares indicated. A share certificate is also referred to as a stock certificate;
    f. A shareholder register, which is a list of active owners of a company's shares, updated on an ongoing basis. The shareholder register requires that every current shareholder is recorded. The register includes each person's name, address, and the number of shares owned;
    g. A shareholder structure, which is the percentage ownership and the percentage of voting rights held by different Shareholders. A company structure can be submitted on the letterhead or in a free format;
    h. The directors register, which is a list of the directors elected by the shareholders, generally stored in the company's minute book;

i. An authorized signatory list, which is a representative with power to sign an agreement (the chairman of the Member of the Board and chief executive officer, the president, the senior vice president and chief financial officer and any executive or senior vice president);
j. A Declaration of Trust, also known as a Deed of Trust, which is a legally-binding document that records the financial arrangements between joint owners of a property, and/or anyone else who a financial interest in the property. A declaration of trust confirms the true ownership of a property in the proportions contributed by each party.

42. Walluta Europe verifies that any person purporting to act on behalf of the legal person / entity is properly authorized.
43. When all required documents are received from the Customer, the AML Specialist shall perform a Customer's documents verification against the personal identity verification and document verification systems provided by Tangany GmbH.
44. The AML Specialist using the personal identity verification and document verification systems provided by Tangany GmbH shall perform the following checks:
    a. Document Integrity checks, automatically verification of the authenticity of photos and scanned copies of physical documents check. The documents Document Integrity checks means analysis of any image or series of images for signs of tampering or modification through the use of graphic editors. Each reviewed document receives a trust score;
    b. Text recognition, allows automatically extract data from the documents;
    c. Additional check. Includes checking of completeness of documents, check if photos have been retaken from a screen or not, cross checking of all data from all submitted documents (name, date and place of birth, signature), checking for duplicated accounts, address check.
45. If AML Specialist detected any problems with verification documents, AML Specialist shall:
    a. if the verification of documents indicates that the identity document may be invalid, the AML Specialist shall contact the issuing authority of the identity document and establish the status of the identity document;
    b. if the identity document is invalid, the AML Specialist shall be notified and establishment of Business Relations with the Customer shall be refused;
    c. verify the data contained in the documents submitted to Walluta Europe by legal entities with the relevant information about them in the databases: for example in the Republic of Poland it will be National Court Register - https://ekrs.ms.gov.pl/
46. Natural persons acting on behalf of the Customer (UBO, directors, etc.) are checked automatically as part of the general KYC process. Checking process includes a combination of state and other public registers, corporate documents provided by the legal entity, and open sources is used. First, basic information about the company is collected (registration number, address, etc.); then a control and beneficial ownership structure is checking with a simultaneous verification of the uploaded documents for the validity and availability of all necessary details. The list of documents that the partner accepts depend from the jurisdiction of the legal entity. Additionally, AML-screening is automatically carried out (check against sanction lists, adverse media, blacklisting, etc.).
47. The respective Customer's excerpt from the register shows the actual authorized representatives of a company in order to ensure that the extract really is up-to-date, it should not be older than 6 (six) months. If the present register extract is older, the AML Specialist must verify its content online. The AML Specialist

must compare the information available in register extract with the information received from the Customer.

48. The AML Specialist contact the Customer to establish the reason of discrepancies, if the verification reveals any discrepancies. The AML Specialist shall refuse establishment of the business relations with the Customer unless the Customer is able to provide logical and reliable explanation of the reasons of such discrepancies.
49. The AML Specialist verify the data contained in the documents submitted to Walluta Europe by legal entities (Customers from other countries if the relevant information about them is available from the European Business Register) against the information contained in the European Business Register database https:// www.ebr.org or other foreign registers available to Walluta Europe.
50. Data from the registers (databases) in question shall be printed out as a part of verifications described above and shall be saved in form of electronic Customer files in the Walluta Europe system.

Identification of Beneficial owner

51. Walluta Europe takes measures to identify the beneficial owner(s) of the contractor and verify his identity by obtaining data stipulated in point 28 of this Policy.
52. Where business relationships are established or occasional transactions are conducted with a contractor which is the entity obligated to register of information on beneficial owners, Walluta Europe shall obtain the confirmation of the registration or a copy from the Polish Central Register of Beneficial Owners or the relevant register maintained in a Member State.
53. Beneficial owner shall be understood as a natural person or natural persons who control, whether directly or indirectly, a contractor through their powers which result from legal or factual circumstances and enable exerting a decisive impact on a contractor's acts or actions, or a natural person or natural persons on whose behalf business relationships are being established or an occasional transaction is being conducted, including:
    a. in the case of a contractor being a legal person other than a company whose securities are admitted to trading on a regulated market that is subject to disclosure requirements market that is subject to disclosure requirements in accordance with the EU law or subject to equivalent third country law:
        i. a natural person being the contractor's shareholder or stockholder and holding the ownership right to more than 25 per cent of the total number of stocks or shares of such legal person, - a natural person holding more than 25 per cent of the total number of votes in the contractor's decision-making body, also as a pledgee or usufructuary, or under arrangements with other holders of voting rights,
        ii. a natural person exercising control over a legal person or legal persons holding in aggregate the ownership right to more than 25 per cent of the total number of stocks or shares of the contractor or holding in aggregate more than 25 per cent of the total number of votes in the contractor's body, also as a pledgee or usufructuary, or under arrangements with other holders of voting rights,
        iii. a natural person holding a senior management function in the case of the documented inability to determine beneficial owner in other way.

b. in the case of a contractor being a trust: - the settlor, - the trustee, - the supervisor, if any, - the beneficiary, - other person exercising control over the trust;
c. in the case of a contractor being a natural person carrying out economic activity with respect of whom/which no premises or circumstances were found which could indicate that any other natural person or natural persons exercise control over him/her, such contractor shall be assumed to be the beneficial owner at the same time.

54. Identification of the Beneficiary serves the purpose of preventing the provision of services by Walluta Europe to one or more natural or legal entities that intentionally and purposefully conceal their actual identity, i.e., under the guise of another natural or legal entity.
55. The AML Specialist shall identify the Beneficiary before establishment of business relations by means of obtaining the minimum information listed in clause 28, in any of the following ways:
    a. Obtaining the information about the Beneficiary of the Customer from Walluta Europe system;
    b. Using the data or documents from the information systems of the Republic of Poland or another country, in particular information from Polish Central Register of Beneficial Owners: https://crbr.podatki.gov.pl/, however Walluta Europe shall not rely exclusively on the information from the Polish Central Register of Beneficial Owners or the register referred to in Article 30 or 31 of Directive 2015/849 maintained in the relevant Member State;
    c. Establishing the identity of the Beneficiary based on the documents proving the identity of a Beneficiary, the document containing up-to-date particulars from the excerpt from the relevant register or other documents, particulars or information originating from a reliable or independent source.
56. In accordance with the provisions hereof, the Responsible Officer shall take all and any steps required, useful, feasible and reasonable to identify the Beneficiaries of the potential and existing Customers. The AML Specialist shall identify the Beneficiary of the Customer as well as the Beneficiary from one or more related financial transactions if different from the Beneficiary identified earlier.
57. The AML Specialist shall perform the steps again described in the AML Policy for identification of the Beneficiary whenever there are grounds to suspect that:
    a. The Beneficiary is a person other than that declared by the Customer; or
    b. The Customer has provided incorrect, inaccurate or incomplete information to Walluta Europe about the Beneficiary.
58. Further, guided by considerations of reasonability, proportionality and usefulness on each individual occasion, and where the circumstances mentioned in clause 57 exist, the AML Specialist shall request one or more of the following documents (information) about the Beneficiary as appropriate on the given occasion:
    a. Information about the Beneficiary's occupation, profession, professional experience and the documents that support such information;
    b. An identification document of the Beneficiary signed by the Beneficiary to certify the status of Beneficiary of the Customer;
    c. A document signed by the Beneficiary to disclose the origin of their Assets and documents that support the legitimacy of the origin thereof (such as certifications from various property registers (the Land Register; the Register of Water Transport Vehicles; the Register of Road Transport Vehicles; the Aircraft Register; the Company Register, etc.), certificates issued by Tax Administration; loan agreements; last wills; current account statements and other documents);

d. Documents supporting the information about the grounds on which the person in question should be treated as the Beneficiary of the Customer (such as current account statements that evidence benefitting from the Customer; reliable written explanation made by the Customer or the Beneficiary to the effect that the Beneficiary benefits from the Customer);
e. Tax (income) returns; certificates of wages, dividends or income from existing contract agreements;
f. Other information and documents about the Beneficiary found appropriate to establish that the declared Beneficiary is the actual Beneficiary.

59. If the AML Specialist finds it appropriate, the AML Specialist may:
    a. request the Beneficiary to appear to Walluta Europe in person and provide the data specified in the AML Policy; or
    b. arrange the AML Specialist's visit to the Beneficiary for obtaining the data specified in the AML Policy; or
    c. obtain further information about the Beneficiary from the sources available to Walluta Europe, such as public databases or the Internet.
60. Having examined the information provided by the Customer and available from other sources about the declared Beneficiary, the AML Specialist shall check and assess the following:
    a. whether such information is sufficient and reliable (the considerations of sufficiency and reliability shall be documented with objective substantiation), that is, whether it is clear from the documents contained in the Customer's file that the Beneficiary is a person corresponding with the economic or personal activities of the Customer (in terms of scope and specifics);
    b. whether it demonstrates that the declared Beneficiary can be the actual Beneficiary;
    c. whether the age or social/financial condition or occupation of the Beneficiary corresponds with the specifics of economic activity of the Customer and raises no suspicion of Money Laundering or Terrorism Financing;
    d. whether the collected information otherwise raises suspicion of Money Laundering or Terrorism Financing.

Business relations with Politically Exposed Persons (PEP)

61. Politically exposed persons (PEP)shall be understood as natural persons with prominent posts or prominent public functions, including:
    a. heads of State, heads of government, ministers, deputy ministers, secretaries of state, and undersecretaries of state, including the President of the Republic of Poland, the Chairman of the Council of Ministers, and the Vice-Chairman of the Council of Ministers;
    b. members of parliament or similar legislative bodies, including deputies and senators;
    c. members of the governing bodies of political parties;
    d. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except under exceptional procedures, including the judges of the Supreme Court, of the Constitutional Tribunal, of the Supreme Administrative Court, of voivodeship administrative courts and judges of appellate courts;
    e. members of courts of auditors or of the management boards of central banks, including the President and members of the Management Board of NBP;
    f. ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

g. members of the administrative, management or supervisory bodies of state-owned enterprises, including directors of state-owned enterprises and members of the management or supervisory boards of companies with the State Treasury shareholdings in which more than a half of stocks or shares are held by the State Treasury or other state-owned legal persons;
h. directors, deputy directors and members of the bodies of international organizations or persons performing equivalent functions in these organizations;
i. general directors of supreme and central offices of state authorities, general directors of voivodeship offices, and managers of field offices of the special government administration authorities.

62. Family members of a politically exposed person - this shall be understood as:
    a. a spouse or a cohabitant of a politically exposed person;
    b. a child of a politically exposed person and his/her spouse or a cohabitant;
    c. parents of a politically exposed person.
63. Persons known to be close associates of a politically exposed person - this shall be understood as:
    a. natural persons who have beneficial ownership of legal persons, organizational units having no legal personality or trusts with a politically exposed person, or any other close relationships with such a person related to the business activity conducted;
    b. natural persons who have sole beneficial ownership of legal persons, organizational units having no legal personality or a trust which is known to have been set up for the de facto benefit of a politically exposed person.
64. In order to establish whether a natural person Customer or a beneficial owner is a PEP Walluta Europe executes determinations as follows:
    a. receives a statement from the Customer or beneficial owner in written or document form, to the effect that the Customer/beneficial owner is or is not a politically exposed person, which statement shall be submitted under pain of penalty of perjury. The person submitting the statement shall include therein the clause reading as follows: “I am aware of the penalty of perjury.”. This clause according to Polish law replaces a notice of penalty of perjury;
    b. check Customer and beneficial owner status in:
        i. https://www.worldpresidentsdb.com/
        ii. https://www.europarl.europa.eu/portal/en
        iii. https://everypolitician.org/
        iv. https://pl.wikipedia.org/wiki/Wikipedia:Strona_g%C5%82%C3%B3wna
        v. https://dilisense.com/
        vi. LexisNexis® WorldCompliance™ Data
    c. check Customer and beneficial owner status with assistance of partner

Enhanced security measures

65. Walluta Europe undertakes enhanced financial security measures in the cases of
    a. higher risk of money laundering or terrorist financing;
    b. business relations with Politically Exposed Persons (PEP)
66. A higher risk of money laundering and terrorist financing can be indicated in particular by:
    a. establishment of business relationships in unusual circumstances;
    b. the fact that the Customer is:

i. a legal person or an organizational unit having no legal personality, whose activity serves to storage of personal assets;
ii. a company in which bearer shares were issued, whose securities are not admitted to organized trading, or a company in which the rights attached to shares or stocks are exercised by entities other than shareholders or stockholders;

c. the subject of the business activity carried out by the Customer covering conducting of a significant number of cash transactions or cash transactions of high amounts;
d. unusual or excessively complex ownership structure of the Customer, having regard to the type and scope of the business activity conducted by this Customer;
e. the fact of the Customer making use of services or products offered as part of private banking;
f. the fact of the Customer making use of services or products contributing to anonymity or hindering the Customer's identification, including the service consisting in creating additional numbers of accounts marked pursuant to the provisions issued under Article 68, subparagraphs 3 and 4 of the Act of 29 August 1997 – Polis Banking Law, as well as Article 4a, paragraph 5 of the Polish Act of 19 August 2011 on Payment Services linked to the account held, in order to make the account numbers available to other entities for the purpose of identification of payments or originators of those payments;
g. the fact of establishment or maintenance of business relationships or conducting an occasional transactions without the Customer being physically present - in the case when a higher risk of money laundering or terrorist financing related thereto was not mitigated in another manner, including by the use of the a notified electronic identification measure adequately to the medium security level referred to in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73) or the requirement of using a qualified electronic signature or a signature confirmed by the Electronic Platform of Public Administration Services (ePUAP) trusted profile;
h. the fact of ordering of transactions by third entities unknown or not linked to a Customer, the beneficiary of which transactions is the Customer;
i. the fact of covering by business relationships or transactions of new products or services or offering of products or services with the use of new distribution channels;
j. linking business relationships or an occasional transaction by Customer with:
    i. a high-risk third country;
    ii. a country defined by reliable sources as a country of high corruption or other criminal activity levels, a country providing funding or support for committing activities of a terrorist nature, or with which an activity of an organization of a terrorist nature is associated;
    iii. a country in relation to which the United Nations Organization or the European Union have taken a decision on imposing sanctions or specific restrictive measures.
k. the fact that business relationships or occasional transaction are related to crude oil, arms, precious metals, tobacco products, cultural artefacts, ivory, protected species or other items of archaeological, historical, cultural and religious importance, or of rare scientific value;
l. the fact that business relationships or occasional transaction are related to a Customer who is a citizen of a third country and applies for a right to stay or citizenship in a Member State in

exchange for capital transfers, immovable property acquisition or Treasury bonds or, as the case may be, investments in corporate entities in a given Member State.

67. Enhanced security measures provides a greater level of scrutiny of potential and current Customers. In the cases of higher risk of money laundering or terrorist financing Global Trade Research undertakes steps to understand the origin and legitimacy of the Customer's wealth and ask Customer for additional documents and information other than stipulated in point 28-33 of the Policy, in particular:
    a. Official corporate records of amendments in corporate structure from last 18 months;
    b. Copy of Annual Financial Statements from last 3 years;
    c. Copy of Tax Declarations with confirmation of submission from last 3 years;
    d. Names and location of Customer's Customers and suppliers;
    e. Bank statements from last 18 months;
    f. Copy of lease agreement of register office;
    g. Standard documents, which confirm the sale of property, inheritance, salary, etc.
68. In the cases of higher risk of money laundering or terrorist financing Walluta Europe verifies also Customer (its representatives and beneficial owner) in sanctions list, in particular:
    a. Warning of The Polish Financial Supervision Authority;
    b. Warnings of the Polish Office of Competition and Consumer Protection ;
    c. VIES – European Comission;
    d. United Nations Security Sanction list;
    e. Us Consolidated Sanctions,
    f. EU Financial Sanctions,
    g. UK Financial Sanctions,
    h. Interpol Wanted List,
    i. Office of the Superintendent of Financial Institutions (Canada)
    j. https://www.un.org/securitycouncil/
    k. https://sanctionssearch.ofac.treas.gov/
    l. https://eeas.europa.eu/headquarters/headquarters-homepage_en
    m. https://eur-lex.europa.eu/
    n. https://www.sanctionsmap.eu/#/main

Monitoring ongoing business relationship

69. Walluta Europe undertakes ongoing monitoring of Customer's business relationship, including:
    a. the analysis of transactions carried out throughout the course of business relationship in order to ensure that such transactions are compliant with the knowledge of Walluta Europe on the Customer, the type and scope of activity carried out by it, as well as compliant with the money laundering and terrorist financing risk associated with such a Customer,
    b. examining the origin of assets available to the Customer - in cases justified by circumstances,
    c. censuring that any possessed documents, data or information concerning the business relationship shall be updated on an on-going basis.
70. Walluta Europe shall perform Customer monitoring compliance with legal requirements and follow the principle Know Your Customer (KYC) in order to minimize to as far as possible the eventual occasions of money laundering and terrorism financing.

71. Customer monitoring shall be performed by the AML Specialist in cooperation with all Employees who are entrusted to performing such duties in accordance with the Internal Regulatory Documents.
72. Customer monitoring shall take the form of:
    a. Monitoring and control of the Customers financial transactions;
    b. Regular supplementing and updating the Customer files;
    c. Regular supplementing and updating the Customer information in Walluta Europe system;
    d. contact with the Customers;
    e. On other affairs specified in the Internal Regulatory Documents.
73. Customer monitoring through the control and monitoring of the Customers financial transactions should be performed under AML Policy. Each day the AML Specialist shall select the Customers for performing outgoing monitoring.
74. The AML Specialist shall review the Customer identification under AML Policy if:
    a. Identification data of the Customer have changed;
    b. Name, surname, personal number of a natural person has changed;
    c. Name, registration number, legal status of a legal entity has changed;
    d. A new identity document has been issued to a natural person;
    e. A new legal corporate document has been issued to a legal entity;
    f. Legal or contractual representative of the Customer has been changed;
    g. There are basis for doubting in the validity of the representation right of legal or contractual representative of the Customer.
75. Customers ongoing monitoring and updating documents/information in the Customer file shall be conducted, depending on the category or status of the Customer:
    a. for the High Risk Customers - at least every quarter;
    b. for the other category risk of Customers - at any time chosen for the Customer by the AML Specialist with due regard to the actual circumstances;
    c. The AML Specialist shall control the regular updates of documents/information in the Customer file, and other Employees shall be attracted in the process as appropriate in the manner prescribed by the AML Policy and the Internal Regulatory Documents.
76. The AML Specialist must update the Customer file according to the following steps:
    a. Review the Customer file;
    b. Check the Customer data in the Company System;
    c. To get overview of financial transactions in the Company System ordered or performed by the Customer during the reporting period.
77. Under the Customer file review, the AML Specialist shall ensure that the Customer file contains all documents and information required in accordance with the AML Policy and Internal Regulatory Documents.
78. Under checking the Customer data in Walluta Europe system, the AML Specialist shall:
    a. ensure that the Customer file contains all required information regarding the Customer;
    b. ensure that all included information corresponds to the documents contained in the Customer file.
79. The AML Specialist shall check the Customer data with focus on the following information:
    a. To which category the Customer belongs to;
    b. The declared economic activity of the Customer;

c. The declared amounts of financial transactions performed by the Customer;
d. The partners and geographic regions of economic activity of the Customer.

80. Under checking the Customer file and Customer's financial transactions report (the report should be stored in electronic format in the Customer file), the AML Specialist shall prepare the assessment or opinion.
81. Under the assessment or opinion on the Customer, the CMD officer shall issue any of the following decisions:
    a. Continue the previous business relationship with the Customer;
    b. Continue the previous business relationship with the Customer and request to submit the following documents and information;
    c. Propose termination of business relationship with the Customer.
82. If the CMD officer makes the decision to continue the business relationship with the Customer and assign the status of high risk to the Customer, further documents or information shall be requested from the Customer to the extent required in accordance with the Internal Regulatory Documents from Customers accordance with the given category.
83. If the CMD officer makes the decision for termination of the business relationship with Customer, business relationship with the Customer shall be terminated in accordance with this AML Policy.
84. If Walluta Europe sends the notice to the Customer with request for documents/information it shall be clearly formulated with questions related to its research and understanding of the Customer's economic or personal activity, for establishing and identification of the Customer's Beneficiary and for taken the decision about business relationship with the Customer.
85. Customers which turnover is equivalent or more than EUR 30.000 shall submit to Walluta Europe a written confirmation of legitimacy of origin of its capital or assets including description of the sources of origin by the request of the AML Specialist.
86. The AML Specialist shall prepare the request for information including the following data:
    a. The Walluta Europe’s forms which to be filled by the Customer;
    b. Link to the access to such forms by the Customer;
    c. Any other documents or information to be submitted by the Customer to Walluta Europe;
    d. The Walluta Europe 's questions to the Customer;
    e. The manner of the Customer's reply to the request;
    f. The period for replying to the request.
87. The period for replying on the request for submitting the documents and information shall be 10 (ten) working days from the request date.
88. The period specified in clause 87 above may be extended or reduced if the CMD officer finds it necessary and feasible.
89. If the request for documents and information is prepared, the CMD officer shall ensure that the term for submitting the documents and information specified in the request is observed.
    a. The Customer may submit the documents and information to Walluta Europe:
    b. via Walluta Europe system;
    c. by e-mail;
    d. in person to Walluta Europe.
90. After Customer reply with requested documents and information is received, the AML Officer shall immediately (within the next following business day) check:

a. Does the Customer has performed all requirements specified in the request for submitting of documents and information, including: all necessary forms are filled out; all requested information and documents submitted; all answers on the questions are submitted.
b. Does the form comply with documents submitted by the Customer and perform the requirements of regulatory acts and the Internal Regulatory Documents concerning the executing of documents.

91. If Customer submitted documents and information does not comply with all requirements specified in the request, with regulatory acts and the Internal Regulatory Documents, the AML Specialist shall request to the Customer to correct identified deficiencies within three business days and immediately notify the AML Officer (within the next following business day) by e-mail.
92. If the Customer does not comply with requirements under request for remove of the identified flaws, the AML Officer shall immediately (next business day after following to expiration period granted for replying on the request and for presentation of information and documents) forward the documents received from the Customer in the volume and form received by the AML Officer on the period expiration day for provided for replying to the request for submitting the documents and information.
93. If the Customer does not comply with requirements under request for documents and information under specified period or fails to meet the request for elimination of the identified shortcomings within the specified period, the AML Specialist shall e-mail a report on such fact to the AML Officer, along with the documents submitted by the Customer, and specify the following:
    a. The date and delivery method of the request for documents\information to the Customer;
    b. The period for providing the reply on the request for documents and information or remove of the identified flaws;
    c. Any reasons for not fulfilling answer deadline from the Customer site.
94. The AML Officer should receive the reply with the requested documents and information from the Customer, if establish the failure of the Customer in presenting the requested documents or their insufficiency or non-compliance with the Walluta Europe 's requirements, the AML Officer shall take the following steps:
    a. Issue additional request for documents and information to the Customer specifying the additional documents to be submitted by the Customer to Walluta Europe and the term for answering to the request for documents and information;
    b. Issue request for documents and information to the Customer in accordance with the AML Policy.
95. The AML Specialist shall remind, if Customer does not answer to the request for documents and information and ensure that all requirements are performed, the AML Specialist shall obtain approval with allocated instruction from the CMD officer (using the “reply” function via e-mail).
96. Monitoring also involves identifying expired documents, changes in company structures, changes in address or business location and determining whether the Customer has become politically exposed, sanctioned or involved in dealings which are deemed to be high risk. Changes in the Customer profile might increase the Customer’s risk category assigned, therefore requiring enhanced security measures.

Screening of transactions

97. The AML Specialist or AML Officer should check the ordered and performed transactions of the Customers for detecting suspicious transactions.

98. In accordance with the AML Policy and Internal Regulatory Documents the AML Specialist or AML Officer should perform the following steps:
99. Real-time screening;
    a. Retroactive searching;
    b. Transaction monitoring.
    c. Real-time screening mean screening of a transaction before performing.
100. Real-time screening should be performed is aimed to prevent the access to the Company services by any person what could be subject to the international and national sanctions.
101. Automatic real-time screening should be performed, if:
    a. Walluta Europe`s system issues a warning to the AML Specialist or AML Officer who accepts the transaction, therefore he or she should check the information included in the transaction details with the warning or sanctions lists;
    b. The AML Specialist or AML Officer should check the warning assess the coincidence and proceed with the steps prescribed in the AML Policy regarding to suspicious transactions, if the name and surname of the person or name of the company matches or differ from the name and surname of the respective person, or name of an organization contained in the matches lists by 3 or less digits.
102. Retroactive searching means early performed transaction screening.
103. Retroactive searching shall be conducted by the AML Specialist in cooperation with other Employees for the purpose of analysis of the Customer on the basis of the transactions ordered or performed by the Customer.
104. Retroactive searching shall be conducted:
    a. Through Walluta Europe system where the information is saved about all and any transactions ordered/performed by the Customer;
    b. By the AML Specialist via e-mail request for information regarding the transactions or from the Employees which is performing Customer support;
    c. By the AML Specialist through the search functions of Walluta Europe system;
    d. By the AML Specialist using the reporting function in Walluta Europe system that allows different report printing in respect of the Customers, transactions or groups of Customers from Walluta Europe system according to specified criteria.
105. The AML Specialist shall request information via e-mail about the transactions of interest from the Employees who perform Customer support, where it is appropriate and execute the request in writing.
106. Before receiving the request from the AML Specialist about transactions, the Employee who performing Customer support shall replay via e-mail received request within the period specified in such request.
107. The request issued by the AML Specialist, replies and analysis received from other Walluta Europe Employees shall be stored in electronic format in the Customer file.
108. Transaction monitoring means the monitoring of an individual transaction or a series of transactions aimed at preventing Money Laundering and Terrorism Financing.
109. Transaction monitoring shall include assessment of relation of the Customer's economic or personal activity and financial condition with the nature and amount of the transaction and ensuring that the transaction neither meets the criteria of suspicious transaction nor raises suspicion of Money Laundering or Terrorism Financing.

110. Transaction monitoring shall be provided by means of the various filters integrated in Walluta Europe system before performing the transaction and as a part of their analysis after the performance. The types of filters, what should be integrated into Walluta Europe system (such as filters for each individual type of electronic funds or virtual currency) shall be defined and documented by the Member of the Board of Walluta Europe. Integration of the filters defined by the Member of the Board of Walluta Europe into the Walluta Europe system shall be ensured by the IT department.
111. The filters integrated in Walluta Europe system shall be enable the Employees to focus on transactions exposed to higher risk and subject to manual treatment prior to their performance.
112. The features and criteria for the filters, which should be integrated into Walluta Europe system shall be developed by the AML Officer or Member of the Board of Walluta Europe in cooperation with the IT department.
113. Special attention before accepting of the ordered transactions shall be given to the following transactions:
    a. Large, complicated transactions on typical for the Customer or series of transactions without evident economic or legitimate purpose;
    b. Transactions with participation of parties from the Third Countries listed according to the opinion of the international bodies as jurisdictions with non-existing or weak regulatory acts for Anti Money Laundering or Terrorism Financing or countries that have refused to cooperate with the international bodies in the area of Anti-Money Laundering and Terrorism Financing.
114. In case of uncertainty or doubt, Employee, who is responsible for compliance assessment of transactions shall be available to request written approval for payment or separate written opinion regarding the transaction from AML Officer or Member of the Board of Walluta Europe.

Termination of business relations with the Customer

115. Should Walluta Europe be unable to apply one of the Customer due diligence measures:
    a. it shall not establish a business relationship;
    b. it shall not perform an occasional transaction;
    c. it shall not conduct transactions through the bank account;
116. Walluta Europe must terminate business relations with the Customer according to AML Policy and other Internal Regulatory Documents.
117. If identification of the Customer is required by the Anti-Money Laundering and Terrorism Financing Law, but identification of the Customer and the Beneficiary in accordance with the AML Policy is impossible, the AML Specialist shall not allow the service for such persons, establish business relations and perform financial transactions with such persons; the AML Specialist shall terminate the business relations with Customer.
118. The AML Specialist must terminate business relations with the Customer if identification of the Customer or received information and documents in the volume required to enable the relevant investigation of the Customer is not possible. The AML Specialist in collaboration with the Member of the Board of Walluta Europe shall also decide to terminate of business relations with other Customers that have the same Beneficiaries, or on early enforcement of such Customer's obligations.
119. Walluta Europe must decide about termination of business relations with the Customer if minimum due diligence requirements regarding Customer cannot be performed within 14 days before establishment of the preconditions to due diligence of the Customer.

120. The AML Specialist shall prepare a draft decision (in electronic format) about termination of business relations (Business Relations with Walluta Europe or performance of financial transactions) with the Customer and present such draft to the Member of the Board Member of Walluta Europe on the following occasions:
    a. The Customer does not perform the requirements of Internal Regulatory Documents in accordance with the applicable regulatory acts of the Republic of Poland.
    b. The Customer does not submit to Walluta Europe complete data as requested or provide incorrect data or evidently falsified documents, or otherwise attempts to deceive Walluta Europe.
    c. According to the information available by Walluta Europe, the Customer is involved in fraudulent transactions, Money Laundering or Terrorism Financing, or the Customer, its legal or contractual representative or the Beneficiary, or a person otherwise related to the Customer is likely to expose Walluta Europe to increased legal, reputation or other risk.
    d. The Customer or persons related to it (legal or contractual representatives, the Beneficiaries, etc.) are among the persons in respect of which Walluta Europe abstains from cooperation.
    e. The Beneficiary can't provide to Walluta Europe additional information by Walluta Europe request without important reason.
    f. On the occasions described in clauses 74 and 75.
121. Business relations with the Customer shall be terminated based on the decision approved by Walluta Europe in accordance with the AML Policy and Internal Regulatory Documents or by the Customer's initiative.
122. Walluta Europe has the right to take decision about termination of the business relations approved on the grounds of the Internal Regulatory Documents specifying the following:
    a. Walluta Europe decision with reference to the applicable Internal Regulatory Documents, as well as to the clause of agreement entered with the Customer and/or to the regulatory act (for example, the Anti-Money Laundering and Terrorism Financing Law) that permits the implementation of such decision.
    b. Date of such decision is taken.
    c. Date of termination of business relations with the Customer.
    d. Restrictions imposed on the Customer when Customer performing financial transactions provided by the Company and the ordering/performance of financial transactions.
123. Decision about business relations termination with the Customer shall be approved by the Member of the Board or CMD officer of Walluta Europe.
124. Decision about termination of business relations with the Customer shall be implemented as follows:
    a. The AML Officer shall immediately take all necessary steps to terminate business relations with the Customer and block the Customer account in Walluta Europe system at the time specified in the decision.
    b. The AML Officer, which is responsible for preparing the respective draft decision shall notify all related Employees about the possibility of performing the financial transactions by the Customer and inform about taken decision via e-mail.
    c. The Customer and related persons must be entered into Walluta Europe 's Blocked Client list, if termination of business relations with the Customer is a result of material breach on the part of the Customer.

d. The AML Specialist shall immediately notify the Customer about the decision approved in accordance with AML Policy.

125. If Employee, who is responsible for Customer service, after implementation of the instruction for termination business relations with the Customer within the prescribed period is prevented by contractual or overdue obligations on the part of Walluta Europe or the Customer, the Employee shall immediately report about such a fact via e-mail form to the AML Specialist that has prepared the decision on termination of cooperation, and the latter shall upon receipt of such report prepare a draft decision either on prolongation of the period for termination of cooperation or on early termination of obligations and present such draft to a Member of the Member of the Board of Walluta Europe for approval of decision.
126. Business relations with the Customer shall be terminated in the same day until the end of the working day after decision about business relations with the Customer was notified, unless other period is prescribed by the AML Policy.
127. If decision about termination of business relations with the Customer is approved by Walluta Europe on the basis of suspected involvement of the Customer in Money Laundering or Terrorism Financing, or fraud, business relations with the Customer shall be terminated immediately.
128. The Member of the Board of Walluta Europe shall prescribe other periods for termination of business relations if the AML Specialist that has drafted the decision about termination of business relations with the Customer finds it necessary and feasible.
129. The AML Officer, who prepare a draft decision about termination of business relations with the Customer shall be available on the basis of such decision to impose restrictions on the financial transactions performing by the Customer via Walluta Europe during the period from the approve of such decision and the termination of cooperation.
130. If the AML Specialist receive the appropriate approval with instructions from the AML Officer via e-mail (using the “reply” function), AML Specialist shall save the approval received from the AML Officer in the electronic format in the Customer file and activate in Walluta Europe system the function that prohibits the Employees (in the manner stipulated in the agreement entered into with the Customer) to perform financial transactions for the Customer; the AML Officer shall notify the Employee that services the Customer in question thereof in form of e-mail.
    a. The restrictions shall be imposed for the following conditions:
    b. The Customer category to which the Customer belongs;
    c. The basis for termination of business relations;
    d. Walluta Europe 's experience from cooperation with the Customer in question;
    e. Other condition that may be relevant for accepting the appropriate decision.
131. Walluta Europe shall assess whether the inability to apply the Customer due diligence measures forms basis for providing the GIIF with the notification referred to in Article 74 or Article 86 of Polish AML Act.

Record keeping

132. The Customer file shall include all documents and information executed in accordance with AML Policy and contains identification data of the Customer, the documents as evidence of the legal capacity and competence of the Customer and their representatives, other documents shall be stored in the Customer File in accordance with the AML Policy and other Internal Regulatory Documents.
133. The Customer File shall include:

a. All documents received from the Customer, as well as the documents executed by Walluta Europe in relation to the Customer.
b. Electronic versions of the Customer Files at Walluta Europe information system including received/executed documents or information in electronic format (such as information tiled in Walluta Europe system, e-mail messages, etc.).

134. The AML Specialist shall be responsible for storage (in electronic format) of the following documents in the Customer File, either initially submitted by the Customer or additionally received at any other time:
    a. All and any documents to be received and executed for the opening and subsequent operation of the Customer profile:
        i. Passport, ID card or driving license;
        ii. Address verification document, as utility bill (for gas, water, electricity, TV or Internet); bank statement with address; credit card statement with a list of transactions and address; registration page from national passport with photo;
        iii. The Customer selfie;
        iv. Walluta Europe retains the entire correspondence relating to the performance of the duties and obligations arising from legislation of Republic of Poland and all the data and documents gathered in the course of monitoring the business relationship as well as data on suspicious or unusual transactions or circumstances which the GIIF was not notified of.
    b. Additionally for identity confirmation or identity and resident country confirmation AML Specialist can request:
        i. applications;
        ii. information about Customer source of funds;
        iii. administrative acts of public authorities and officials;
        iv. documents which belongs to the economical, personal or financial activity of the Customer (if required);
        v. materials of internal investigation of the Customer's activity;
        vi. all and any documents received by Walluta Europe under Customer due diligence process in accordance with the AML Policy regarding Customer and Customer's performed transactions and documents submitted by the Customer regarding Customer and Customer's performed transactions.

135. The requirements specified in other Internal Regulatory Documents shall be additionally applied to the Customer Files.

136. Walluta Europe is allowed to process personal data gathered upon implementation to the legislation of the Republic of Poland only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

137. General information on the duties and obligations of Walluta Europe upon processing personal data for AML/CFT purposes is available on Walluta Europe's webpage in Section Privacy Policy.

138. Walluta Europe shall maintain, for the period of 5 years counting from the date on which business relationships with a Customer were terminated or on which occasional transactions were conducted, the following documents

a. copies of documents and the information obtained as a result of application of financial security measures;
b. evidence confirming conducted transactions and records of the transactions, said evidence including original documents and copies of documents necessary for identifying a transaction.

139. Prior to the expiry of the period referred to point a and b of point 94, the General Inspector may demand the storing of the documentation for the subsequent period not longer than 5 years, counting from the day on which the period expires, if this is necessary in order to counteract money laundering or terrorist financing.

AML Officer and reporting

140. Walluta Europe shall appoint senior management members responsible for the performance of the obligations defined in the Polish AML Act. Where a management board or other governing body operates, a person responsible for the implementation of the obligations defined herein shall be appointed among members of such a governing body.
141. Walluta Europe shall appoint the AML Officer - an employee holding a management position, responsible for ensuring the compliance of activity of the obligated institution and its employees and other persons performing activities for this obligated institution with the provisions on money laundering and terrorist financing.
142. The AML Officer is also responsible for submitting, on behalf of Walluta Europe, of the notifications referred to in Article 74, paragraph 1, Article 86, paragraph 1, Article 89, paragraph 1, and Article 90 Polish Act of 1st March 2018 on counteracting money laundering and financing terrorism, that is:
    a. notification the General Inspector of the circumstances which could indicate a suspicion of commission of an offence of money laundering or terrorist financing;
    b. notification the General Inspector, by electronic communication means, of a case of justified suspicion that a given transaction or specific property values may be associated with money laundering or terrorist financing.
    c. notification the competent prosecutor of a case of a justified suspicion that the property values being the subject of a transaction or accumulated on an account are the proceeds of an offence other than an offence of money laundering or terrorist financing or a fiscal offence or are associated with an offence other than an offence of money laundering or terrorist financing or with a fiscal offence.
    d. notification the General Inspector, by electronic communication means, of conducting the suspicion, in the case when provision of the notification was impossible prior to its conducting. In the notification Walluta Europe shall justify the reasons for failure to previously provide the notification and provide the information confirming the suspicion;
143. The AML Officer is responsible also for preparing and submitting quarterly statistical report to the GIIF.
144. Walluta Europe shall provide to the General Inspector the information on:
    a. a received payment or disbursement of the funds of equivalent in excess of EUR 15,000 made;
    b. a transfer of funds of equivalent in excess of EUR 15,000 made, except:
        i. a national transfer of funds from other obliged institution;
        ii. a transaction associated with the obliged institution's business dealings, which was conducted by the obliged institution in its own name and on its own behalf, including a transaction concluded on an interbank market;

iii. a transaction conducted on behalf of or for public finance sector entities referred to in Article 9 of the Polish Act of 27 August 2009 on Public Finance;
iv. a transaction conducted by a bank associating cooperative banks, if the information on the transaction has been provided by an associated cooperative bank;
v. conveyance of ownership for the purpose of securing property values made for the duration of a contract of ownership conveyance with an obliged institution.

145. An obligation of providing of information as referred to in point 143 letter a and b shall refer also to a transfer of funds from outside the territory of the Republic of Poland if the payment service provider is an obliged institution.

146. Walluta Europe shall provide the information within 7 days from the day of:
a. receipt of the payment or making disbursement of funds - in the case of the information referred to in point 143 letter a;
b. execution of a payment transaction in the form of a transfer of funds - in the case of the information referred to in point 143 letter b;
c. making available the recipient's payment means - in the case of the information referred to in point 144.

147. The information shall contain:
a. a unique transaction identifier in the records of Walluta Europe;
b. the date or the date and the time of conducting the transaction;
c. the identification data the Customer giving an instruction or order of conducting the transaction;
d. the amount and currency being the subject of the transaction;
e. the transaction type;
f. the transaction description;
g. the manner of issuing an instruction or order of conducting the transaction;
h. the numbers of the accounts used for conducting the transaction marked with the identifier of the International Bank Account Number (IBAN) or an identifier including the code of the country and the account number in the case of accounts not marked with an IBAN.

148. Walluta Europe shall notify the General Inspector of the circumstances which could indicate a suspicion of commission of an offence of money laundering or terrorist financing.

149. Specific instructions of fulfilling reporting obligations for AML Officer, AML Specialist and Walluta Europe employee are stipulated in Annex No 1 “Reporting Manual”.

Exclusion of entering business relationship by Walluta Europe

150. Walluta Europe is not entering into business relations with Customers from a high-risk third country or having a registered office in such a country. High-risk third country shall be understood as a country identified on the basis of information obtained from reliable sources, including reports from evaluation of national systems of counteracting money laundering and terrorist financing conducted by the Financial Action Task Force on Money Laundering (FATF) and the bodies or organizations associated with it, as not having an effective system of counteracting money laundering or terrorist financing or having strategic deficiencies in its system of combating money laundering or terrorist financing, in particular a third country identified by the European Commission in the delegated act adopted under Article 9 of Directive

2015/849 - https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en

151. On 7 January 2022, the European Commission adopted a new Delegated Regulation in relation to third countries which have strategic deficiencies in their AML/CFT regimesSearch for available translations of the preceding that pose significant threats to the financial system of the Union ('high-risk third countries'). Identification of such countries is a legal requirement stemming from Article 9 of Directive (EU) 2015/849 (4th anti-money laundering DirectiveSearch for available translations of the preceding linkEN and aiming at protecting the Union financial system and the proper functioning of the internal market. The Delegated Regulation amends Delegated Regulation (EU) 2016/1675Search for available translations of the preceding
152. Walluta Europe is not entering into business relations with Customers of US residency.

AML audits

153. Walluta Europe is aware that external audits by qualified AML experts provide a needed degree of objectivity in evaluating the internal controls program. Walluta Europe use services of licensed law firm in Poland, which provides Walluta Europe with a summary judgment about the quality of the Anti-Money laundering program.

Training

154. As part of Walluta Europe Anti- Money Laundering program, all personnel is expected to be fully aware of the Anti- Money Laundering policies. Walluta Europe's employees are obligated to read and comply with this document and sign the acknowledgement form confirming that he has read and understands Anti- Money Laundering policies. Moreover, all personnel is required to reconfirm their awareness of the contents of Anti- Money Laundering policies by signing the acknowledgement form every 4 months.

155. All new employees receive anti-money laundering training as part of the mandatory new-hire training program. All applicable employees are also required to complete AML and KYC training annually. Participation in additional targeted training programs is required for all employees with day-to-day AML and KYC responsibilities.

156. Walluta Europe ensures participation of the persons performing the obligations associated with counteracting money laundering and terrorist financing in training programs covering the execution of those obligations. The training programs take into consideration the nature, type and size of activity conducted by Walluta Europe and ensure up-to-date knowledge in the realm of the discharge of obligations of the obliged institution, in particular the obligations referred to Article 74, paragraph 1, Article 86, paragraph 1 and Article 89, paragraph 1 Polish Act of 1st March 2018 on counteracting money laundering and financing terrorism

157. Walluta Europe's training program Includes, at a minimum:

    a. how to identify signs of money laundering or financing of terrorism that arise during the course of the employees' duties;
    b. what to do once the risk is identified (including how, when and to whom report);
    c. what employees' roles are in Walluta Europe's compliance efforts and how to perform them;
    d. the disciplinary consequences (including civil and criminal penalties) for non-compliance.

158. Walluta Europe's personnel is obligated:

a. At a time specified by the AML Officer, to undertake training programs on anti-money laundering policies and procedures;
b. Participate in training how to recognize and deal with transactions which may be related to money laundering;
c. Timely escalate and report the matter to the AML Officer;
d. To get themselves acquainted with Anti Money Laundering Policy;
e. Direct any doubts or queries in regard of Walluta Europe 'Anti Money Laundering Policy to AML Officer.

Personnel protection

159. Walluta Europe shall develop and implement an internal procedure of anonymous reporting by employees actual or potential breaches of the provisions in the field of combating money laundering and terrorist financing.
160. The procedure for anonymous reporting of breaches referred to in point 50 shall, in particular, specify:
a. the person responsible for receiving the reports;
b. the method of receiving the reports;
c. the manner of protection of an employee, ensuring at least protection against actions of a repressive nature, discrimination or having an impact upon deterioration other types of their legal or actual situation or consisting in directing threats; unfair treatment;
d. the manner of protection of personal data of an reporting employee and the person charged with committing a violation, pursuant to the provisions on protection of personal data;
e. the rules for preserving confidentiality in the case of disclosure of identity;
f. the type and the nature of follow-up actions taken after receipt of the report;
g. the time limit of removal by Walluta Europe of personal data contained in the reports.

161. Walluta Europe shall ensure employees protection against undertaking against them actions of a repressive nature or having an impact upon deterioration of their legal or actual situation or consisting in directing threats.
162. Walluta Europe shall ensure employees performing activities related to fulfillment by the obliged institutions of the duties referred to in Article 74, Articles 86, 89 and 90 Polish Act of 1st March 2018 on counteracting money laundering and financing terrorism protection against undertaking against these persons actions of a repressive nature or having an impact upon deterioration of their legal or actual situation or consisting in directing threats.
163. Walluta Europe shall not undertake against the employees actions of a repressive nature or having an impact upon deterioration of their legal or actual situation or consisting in directing threats against them, in particular actions adversely affecting their working or employment conditions.
164. Employees and other persons performing activities for Walluta Europe exposed to the actions referred to in point 53 shall be entitled to report to the General Inspector the instances of such actions.

This AML Policy was prepared on 29/12/2023 is effective as of this date.

Werner Wildberger

President of the Management Board / Senior Management representative designated for implementing the duties set out in the Polish Act of March 1, 2018 on counteracting money laundering and financing of terrorism

Signature:_____

Annexes:

1. Annex 1 “Reporting Manual”;

2. Annex 2 “Risk Assessment”;

Annex No 1 "Reporting Manual"

Walluta Europe Sp. z o.o. with its registered seat in Lodž
116/52 Piotrowska Street
90-006 Lodž
Republic of Poland
NIP (TIN): 7252327520
REGON (Statistical Number): 524238470
KRS (Commercial Number): 0001014691

§ 1 Introduction

1. Walluta Europe Spółka z ograniczoną odpowiedzialnością with its registered seat in Lodž, Republic of Poland (hereinafter: "Walluta Europe"), is legal entity incorporated by laws of the Republic of Poland and entered into Commercial Register, hold by District Court for the city of Łódź-Śródmieście in Łódź, 20th Commercial Division of National Court Register, with Commercial No. ("KRS" number): 0001014691.
2. The main objective of Reporting Manual is providing appropriate controls for reporting of transactions exceeding threshold limit and suspicious activities in accordance with applicable laws, procedures and regulatory guidelines.
3. This Reporting Manual is revisited periodically and amended from time to time (especially in relation to changes in the risk factors concerning contractors, countries or geographical areas, products, services, transactions or their delivery channels – according to art. 27 point 3 Polish Act of 1st March 2018 on counteracting money laundering and financing terrorism) based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing.
4. This Policy is subject to approval by the senior management of Walluta Europe.

§ 2 AML Officer and reporting

1. Walluta Europe shall appoint senior management members responsible for the performance of the obligations defined in the Polish AML Act. Where a management board or other governing body operates, a person responsible for the implementation of the obligations defined herein shall be appointed among members of such a governing body.
2. Walluta Europe shall appoint the AML Officer - an employee holding a management position, responsible for ensuring the compliance of activity of the obligated institution and its employees and other persons performing activities for this obligated institution with the provisions on money laundering and terrorist financing. The appointed employee shall be also responsible for the submission of notifications referred to in Article 74(1), Article 86(1), Article 89(1) and Article 90 of Polish AML Act on behalf of Walluta Europe, that is:
    e. information on transactions exceeding threshold limits prescribed in Polish AML Act;
    f. notification the GIIF of the circumstances which could indicate a suspicion of commission of an offence of money laundering or terrorist financing;
    g. notification the GIIF, by electronic communication means, of a case of justified suspicion that a given transaction or specific property values may be associated with money laundering or terrorist financing.

h. notification the competent prosecutor of a case of a justified suspicion that the property values being the subject of a transaction or accumulated on an account are the proceeds of an offence other than an offence of money laundering or terrorist financing or a fiscal offence or are associated with an offence other than an offence of money laundering or terrorist financing or with a fiscal offence.
i. notification the GIIF, by electronic communication means, of conducting the suspicion, in the case when provision of the notification was impossible prior to its conducting. In the notification Walluta Europe shall justify the reasons for failure to previously provide the notification and provide the information confirming the suspicion;

3. The AML Officer is responsible also for preparing and submitting quarterly statistical report to the GIIF.

§ 3 Information on transactions exceeding threshold limits prescribed in Polish AML Act (Article 72 of Polish AML Act)

1. Walluta Europe shall provide to the GIIF the information on:
    a. a received payment or disbursement of the funds of equivalent in excess of EUR 15,000;
    b. transfer of funds exceeding the equivalent of EUR 15,000 from outside the territory of the Republic of Poland;
2. Walluta Europe shall provide the information within 7 days from the day of:
    a. receipt of the payment or making disbursement of funds - in the case of the information referred to § 3 point 1 letter a;
    b. making means of payment available to the recipient - in the case of the information referred to in§ 3 point 2 letter b.
3. For the calculating the deadline referred to in § 3 point 2, the provisions of the Polish Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws of 2018, item 2096, as amended). When calculating the deadline for submitting the above-mentioned information, the day on which the event subject to reporting occurred is not taken into account, therefore the counting of the deadline starts from the day following the event, e.g. if receipt of the payment or making disbursement of funds occurred on 22 July, then the deadline for reporting will expire on 29 July (29 July at 23:59:59).
4. If the end of the deadline for submitting the aforementioned information to the GIIF falls on a day that is a public holiday or on Saturday, the deadline for reporting will expire on the next day that is neither a public holiday nor a Saturday.
5. The information shall contain:
    i. a unique transaction identifier in the records of Walluta Europe;
    j. the date or the date and the time of conducting the transaction;
    k. the identification data prescribed in § 3 point 6 of the contractor giving an instruction or order of conducting the transaction:
    l. available identification data referred to in § 3 point 6 related to other parties of the transaction;
    m. the amount and currency being the subject of the transaction;
    a. the transaction type;
    b. the transaction description;
    c. method of issuing the instruction or order to perform the transaction;;

d. the numbers of the accounts used for conducting the transaction marked with the identifier of the International Bank Account Number (IBAN) or an identifier including the code of the country and the account number in the case of accounts not marked with an IBAN.

6. The data of a the contractor involves providing following information in the case of:
    a. natural person:
        i. name and surname,
        ii. citizenship,
        iii. number of the Universal Electronic System for Registration of the Population (PESEL) or date of birth in the case if the PESEL number has not been assigned, and the state of birth,
        iv. series and number of the document confirming the identity of a person,
        v. residence address,
    b. legal person or an organizational unit without legal personality:
        i. name,
        ii. organizational form,
        iii. address of the registered office or address of pursuing the activity,
        iv. NIP, and in the case of a lack of such a number – the state of registration, the commercial register as well as the number and date of registration,
        v. identification data referred to in point 5 letter a subparagraph i and iii of a person representing such legal person or organizational unit without legal personality.

§ 4 Notification the GIIF of the circumstances which could indicate a suspicion of commission of an offence of money laundering or terrorist financing (art. 74 of Polish AML Act)

1. Walluta Europe shall notify the GIIF of any circumstances which may indicate the suspicion of committing the crime of money laundering or financing of terrorism.
2. The notification shall be submitted immediately, not later than two business days following the day of confirming the suspicion referred to in point 1 by Walluta Europe.
3. The following data shall be provided in the notification:
    a) identification data referred to in § 3 point 6 related to the customer of Walluta Europe providing the notification;
    b) available identification data referred to in § 3 point 6 related to natural persons, legal persons or organizational units without legal personality other than customers of Walluta Europe;
    c) type and value of assets and place of their storage;
    d) number of the account maintained for the customer of Walluta Europe, identified by the IBAN or identification containing country code and account number in case of accounts other than identified by IBAN;
    e) available identification data referred to in § 3 point 5 related to the transactions or their attempted performance;
    f) indicating a state of the European Economic Area the transaction is associated with, if it was conducted under the cross-border activity;
    g) available information concerning the identified money laundering or financing of terrorism risk and a prohibited act from which assets can originate;
    h) justification of providing the notification.

4. In accordance with § 4 point 3 letter h the notification to GIIF should, inter alia, contains a justification. This means that Walluta Europe, in the context of establishing circumstances that may indicate a suspicion of the commission of a money laundering or terrorist financing offence, describes, in particular:
   a) what information and documents were collected prior to the establishment of economic relations (e.g., what business profile of the customer was established, what was the declared frequency of transactions, what was the source of origin of the assets indicated),
   b) what information the obliged institution collected in the course of economic relations (e.g. whether the obtained assets and executed transactions were in line with the established profile of economic activity, whether there were any changes of ownership, whether any circumstances changed the risk assigned to the customer, whether the domestic bank received a communication from the foreign bank regarding the return of funds, and if so - what reason was indicated by the foreign bank),
   c) what financial security measures were applied after the circumstances that might indicate a suspicion of crime were identified and what was their outcome (e.g. whether the client's transactions with selected counterparties were analysed and specific cases were selected for further in-depth analysis),
   d) what actions were taken in relation to the client after establishing the circumstances that could indicate a suspicion of crime, and what was the result (e.g. whether telephone contact was made with the client or the client was obliged to present contracts and invoices, whether the client presented the requested documentation in full or in part),
   e) what information and documents were reviewed after determining the circumstances that might indicate a suspected crime, and what was the outcome (e.g. whether ambiguities were found in contracts and invoices submitted by the client),
   f) what was the impact of the finding of circumstances that might indicate a suspicion of a criminal offence on the business relationship (e.g. whether, as a result of the customer's failure to provide documents, the obliged institution decided not to carry out transactions through the bank account or to terminate the business relationship).

§ 5 Notification to the GIIF of any case of acquiring justified suspicion that the specific transaction or specific assets may be associated with money laundering or financing of terrorism (art. 86 of Polish AML Act)

1. Walluta Europe shall immediately notify the GIIF of any case of acquiring justified suspicion that the specific transaction or specific assets may be associated with money laundering or financing of terrorism.
2. In the notification, Walluta Europe shall provide information available to it, associated with the acquired suspicion and information on the expected time of performing the transaction referred to in point 1. With respect to the notification, the provision of § 4 point 3 shall apply accordingly.
3. Upon the receipt of the notification, the GIIF shall immediately confirm the receipt thereof in the form of an official confirmation of the receipt, containing in particular the date and the time of accepting the notification.
4. Until the time of receipt of the request referred to in point 5, or the exemption referred to in point 6, no longer than for 24 hours counting from the moment of the confirmation of the receipt of the notification referred to in point 3, Walluta Europe shall not perform the transaction referred to in point 1 or other transactions charging the account on which assets referred to in point 1 have been collected.
5. In case of recognizing that the transaction referred to in point 1 can be associated with money laundering or financing of terrorism, the GIIF shall provide Walluta Europe with a request to suspend the transaction

or block the account for no more than 96 hours from the date and time indicated in the confirmation referred to in point 3. Walluta Europe shall suspend the transaction or block the account immediately upon the receipt of such request. In the request, the GIIF shall determine assets subject to the request.

6. The GIIF may exempt the obligated institution from the obligation referred to in paragraph 5 in the case if the available information does not provide grounds to notify the prosecutor of suspected crime of money laundering or financing of terrorism or in the case of recognising that the transaction suspension or account blocking could jeopardise the performance of tasks by the judicial authorities and forces or institutions responsible for the protection of public order, citizens' security or prosecution of perpetrators of crimes or fiscal crimes.
7. The GIIF shall submit the request referred to in point 5 or the exemption referred to in point 6 to the GIIF with the use of electronic communication means.
8. Immediately after the submission of the demand referred to in point 5, the GIIF shall notify the competent prosecutor on a suspicion of committed crime of money laundering or financing of terrorism.
9. Upon receipt of the notification referred to in point 8, the prosecutor may issue the decision to suspend the transaction or block the account for a definite period, no longer than 6 months from the day of receipt of such notification.
10. The decision concerning the suspension of the transaction or the blocking of the account referred to in point 9 can be also issued despite the absence of the notification defined in point 8.
11. In the decision referred to in point 9, the scope, method and time of suspending the transaction or blocking the account shall be determined. The decision may be appealed to the court competent to hear the case.
12. Walluta Europe, on request of the customer issuing the instruction or the order to perform the transaction referred to in point 1, or being the account holder or owner of assets referred to in point 1, may inform such customer about the submission of the request referred to in point 5 by the GIIF.
13. The suspension of the transaction or the blocking of the account shall fall before the expiry of 6 months from the receipt of the notification referred to in point 8 unless a decision on asset seizure or a decision concerning material evidence is issued.

§ 6 Notification to the competent prosecutor of any case of acquiring reasonable suspicion that the assets subject to transaction or collected on the account originate from a crime other than the crime of money laundering or financing of terrorism or a fiscal crime, or are associated with a crime other than the crime of money laundering or financing of terrorism or a fiscal crime (art. 89 of Polish AML Act)

1. Walluta Europe shall immediately notify the competent prosecutor of any case of acquiring reasonable suspicion that the assets subject to transaction or collected on the account originate from a crime other than the crime of money laundering or financing of terrorism or a fiscal crime, or are associated with a crime other than the crime of money laundering or financing of terrorism or a fiscal crime.
2. In the notification, Walluta Europe shall provide information available to it, associated with the suspicion and information on the expected time of performing the transaction referred to in point 1.
3. Until the time of receipt of the decision referred to in § 6 point 4, in any case no longer than for 96 hours from the moment of submission of the notification referred to in point 1, Walluta Europe shall not perform the transaction referred to in § 6 point 1 or any other transactions charging the account on which assets referred to in point 1 have been collected.

4. Within the time limit defined in § 6 point 3, the prosecutor shall issue the decision on institution or refusal to institute the proceedings, immediately notifying Walluta Europe thereof. In the event of institution of the proceedings, the prosecutor shall suspend the transaction or block the account, by way of the decision, for a period not longer than 6 months from the date of receipt of the notification referred to in § 6 point 1.
5. The decision concerning the suspension of the transaction or the blocking of the account referred to in § 6 point 4 can be also issued despite the absence of the notification defined in § 6 point 1.
6. In the decision referred to in § 6 point 4, the scope, method and time of suspending the transaction or blocking the account shall be determined. The decision may be appealed to the court competent to hear the case.
7. The suspension of the transaction or the blocking of the account shall fall before the expiry of 6 months from the issuance of the decision referred to in § 6 point 4 and 5 unless a decision on asset seizure or a decision concerning material evidence is issued.
8. Immediately upon the receipt of the decisions referred to in § 6 point 4 and 7, Walluta Europe shall submit, with the use of electronic communication means, information on the notifications referred to in point 1 and copies thereof to the GIIF.

§ 7 Notification to the GIIF of performing transaction in the event if the submission of the notification prior to the performance of the transaction was impossible (art. 90 of Polish AML Act)

1. Walluta Europe shall immediately notify the GIIF of performing the transaction referred to in § 5 in the event if the submission of the notification prior to the performance of the transaction was impossible. In the notification, Walluta Europe shall justify the reasons of its failure to submit the notification in advance and provides information available to it confirming the acquired suspicion referred to in § 5. The provision of § 3 point 5 shall apply accordingly.
2. Walluta Europe shall immediately notify the competent prosecutor of performing the transaction referred to in § 6 in the event if the submission of the notification prior to the performance of the transaction was impossible. In the notification, Walluta Europe shall justify the reasons of its failure to submit the notification in advance and provide information available to it confirming the acquired suspicion referred to in § 6 point 1. The provision of § 6 point 8 shall apply accordingly.

§ 8 Identification form

1. For the purpose of the first fulfillment of the obligations referred to in § 3, § 4, § 5, § 6 and **§** 7 Walluta Europe shall submit a form identifying the company to the GIIF.
2. The form identifying the obligated institution contains:
    b. name, including determining of the organisational form of the obligated institution;
    c. NIP;
    d. determining of the type of activity carried out by the obligated institution;
    e. address of the registered office or address of pursuing the activity;
    f. name, surname, position, telephone number and address of electronic mailbox of the AML Officer;

g. names, surnames, positions, telephone numbers and addresses of electronic mailboxes of other employees responsible for the implementation of the provisions of the Polish AML Act, whom the obligated institution is willing to indicate for contacts with the GIIF

3. In the case of change of the data referred to in paragraph § 8 point 2 Walluta Europe shall immediately update them.

§ 9 Information requested by GIIF

1. On request of the GIIF, Walluta Europe shall immediately submit or make available any information or documents held, required for the implementation of the GIIF's tasks defined in the Polish AML Act, including those referring to:
    a. customers;
    b. performed transactions in the scope of data defined in § 3 point 5;
    c. type and value of assets and place of their storage;
    d. application of the customer due diligence measure;
    e. IP addresses from which the connection with the informatics system of Walluta Europe took place and times of connections with this system.
2. In the request referred to in § 9 point 1 and 2, the GIIF may indicate:
    a. the deadline and form of providing or making information or documents available;
    b. the scope of information as well as the time limit of its acquisition by the obligated institution in connection with the application of the customer due diligence measure or in connection with specific occasional transactions.
3. The information and documents referred to in § 9 point 1 shall be provided and made available free of charge.

This Reporting Manual was prepared on 29/12/2023 is effective as of this date.

Werner Wildberger

President of the Management Board / Senior Management representative designated for implementing the duties set out in the Polish Act of March 1, 2018 on counteracting money laundering and financing of terrorism

Signature:_____

Annex No 2 “Risk Assesment”

Walluta Europe Sp. z o.o. with its registered seat in Lodž
116/52 Piotrwoska Street
90-006 Lodž
Republic of Poland
NIP (TIN): 7252327520
REGON (Statistical Number): 524238470
KRS (Commercial Number): 0001014691

§ 1
Legal basis

1. This document is prepared on the basis of Article 27 of the Polish Act of March 1, 2018 on counteracting money laundering and financing of terrorism (Polish Journal of Laws 2023, item. 1124, 1285, 1723, 1843 - consolidated text).
2. Following to above mentioned article, Walluta Europe Spółka z ograniczoną odpowiedzialnością with its registered seat in Lodž, Republic of Poland (hereinafter: “Walluta Europe”), as obliged institution, shall identify and assess the risk connected with money laundering and terrorist financing related to its operations, taking account of the factors of risk concerning customers, countries or geographical areas, products, services, transactions or delivery channels. These actions shall be proportionate to the nature and size of the obliged institution.
3. While assessing the risk, Walluta Europe may take into account the binding national risk assessment, as well as the report of the European Commission referred to in Article 6(1)-(3) of Directive 2015/849.
4. The Risk Assessment is prepared by Walluta Europe in hard copy or electronic form and where necessary, however at least once every 2 years, Walluta Europe shall update this assessments, especially in relation to changes in the risk factors concerning customers, countries or geographical areas, products, services, transactions or delivery channels or the documents referred to in paragraph 2.

§ 2
Information sources

Walluta Europe, as an obligated institution, to identify the risk of money laundering or terrorist financing, takes into account, in particular:

1. information contained in the international risk assessments prepared by the European Commission,
2. information included in the national risk assessment prepared by the General Inspector of Financial Information (pl: “Generalny Inspektor Informacji Finansowej”) - “GIIF”
3. information indicated on the website https://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/giif operated by the GIIF,
4. own knowledge and professional experience,
5. information obtained from clients, their proxies or statutory representatives,
6. information disclosed in public registers,
7. information contained in official documents submitted to Walluta Europe.

§ 3
Purpose of risk assessment

1. The purpose of the risk assessment is for Walluta Europe, as an obliged institution, to identify and determine the level of risk related to money laundering and terrorist financing, taking into consideration its professional activity in respect of the business activity as defined in Article 2(1)(13) of the Polish Act of March 1, 2018 on counteracting money laundering and financing of terrorism:
    a. exchange between virtual currencies and means of payment;
    b. exchange between virtual currencies;
2. Risk assessment takes into account the risk factors relating to the client, the beneficial owner, the countries or geographical areas, the type and subject matter of the activity covered by Walluta Europe's business activity.
3. The risk assessment was made taking into account the size of Walluta Europe's undertaking and the nature of its business, which is characterized by:
    a. subject of Walluta Europe's transactions are virtual currencies, which are developing very quickly and are an example of digital innovation. However, at the same time, there is a risk that virtual currencies could be used by terrorist organizations to circumvent the traditional financial system and conceal financial transactions as these can be carried out in an anonymous manner. However, these could be more accurately described as 'pseudonymous'. The nature of distributed ledger technology means that every transaction carried out on a DLT-based system is recorded in multiple locations. Therefore, transactions and owners can ultimately be tracked. The difficulty can then lie in identifying who it is carrying out transactions, particularly when multiple transactions are carried out to obscure a trail. Hence the use of 'mixers' or 'tumblers' which mix potentially identifiable currencies with others so as to make it more difficult to trace those engaged in illicit activities.
    b. virtual currencies are characterized by the lack of a central oversight body;
    c. 5AMLD brought much-needed transparency to the virtual currency sector across the EU;
    d. the price of virtual currencies fluctuates constantly;
    e. the data of the clients are always established and verified on the basis of presented original documents stating identity or scan copies;
    f. there is possibility to perform the transaction in physical absence of the client;
    g. transactions are always financed with funds from client's bank accounts, which means that the client has been additionally verified by an obliged institution other than Walluta Europe;
    h. payments made by the clients are not flexible, i.e. they do not provide for a possibility to pay more than the amount specified in the transaction and later return the overpayment to the paying party or a third party.

§ 3
Money laundering or terrorist financing risk factors

In identifying the risk of money laundering or terrorist financing and assessing the level of such risk, Walluta Europe consider factors relating to:

1) the client;
2) beneficial owner;
3) countries and geographical areas,

Above mentioned factors may be grouped into following criteria:

1) Economic - consisting of assessing the client's transactions in terms of the purpose of its business activity;
2) Geographical - involving transactions not justified by the nature of the business concluded with entities from countries where there is a high risk of money laundering and terrorist financing;
3) Object-oriented - consisting in carrying out by the client of a high-risk business activity from the point of view of vulnerability to money laundering and terrorist financing;
4) Behavioral - consisting of atypical, in a given situation, behavior of the client.

§ 4

Risk factors concerning client and beneficial owner

1. When recognizing the risk of money laundering or terrorist financing and assessing the level of such risk related to the client, Walluta Europe considers:
    a. the profile of the client's professional or business activity, in particular:
        i. whether the client is engaged in virtual currency business activity,
        ii. whether the client is engaged in non-profit activities,
        iii. whether the type or subject matter of the activity covered by the transaction falls within the profile of the client's professional or business activity,
    b. circumstances concerning the person of the client, in particular:
        i. whether there is reasonable doubt as to the identity of the client,
        ii. whether the client is an entity other than a natural person,
        iii. whether the client is a person holding a politically exposed position within the meaning of Art. 2 sec. 2 item 11) of the Polish AML Act or has ceased to hold such a politically exposed position in the last 12 months, or is a family member of a person holding a politically exposed position within the meaning of Art. 2(3) of the Polish AML Act or a person who has ceased to hold such a politically exposed position within the last 12 months, or is a person known to be a close associate of a politically exposed person within the meaning of section 2(2)(12) of the Polish AML Act or a person who has ceased to hold such a politically exposed position within the last 12 months,
        iv. whether the client, whose appearance may indicate that he is not a wealthy person, engages in a transaction of substantial property value,
        v. whether the ownership structure of a client that is a legal entity is transparent,
        vi. whether the client is a person or entity entered by the GIIF on the list of persons and entities subject to special restrictive measures referred to in Chapter 10 of the Polish AML Act,

c. client's behavior during the conducting the transaction, in particular:
    i. whether the client uses a false identity as evidenced by the documents presented,
    ii. whether the client refuses to submit documents within the meaning of Article 37 of the Polish AML Act confirming the identity of the client or real beneficiary, despite the fact that the documents may be submitted by the client without obstacles,
    iii. whether the client intentionally provides data that is inconsistent with reality,
    iv. whether the client demands an unreasonably high level of confidentiality,
    v. whether the customer behaves in an unusual manner (e.g. shows signs of unjustified nervousness or fear),
    vi. whether the client is conducting transaction in the presence of third party, which acts in a suspicious manner,
    vii. whether the client carries out the transaction in the company of a third party who gives him instructions concerning the transaction,
    viii. whether the customer transports a significant amount of money in cash in an unusual manner,
    ix. whether the documents submitted by the client raise reasonable suspicion as to their authenticity,
    x. whether the client refrains from conducting the transaction in the event that Walluta Europe's personnel shows interest in the details of the transaction,
    xi. whether the client does not disclose data allowing identification of the beneficial owner, despite knowing such data,
    xii. whether the client provides information requested by Walluta Europe with undue delay.

2. When recognizing the risk of money laundering or terrorist financing and assessing the level of this risk related to the beneficial owner, Walluta Europe takes into account the circumstances concerning the person of the beneficial owner, in particular:
    a. whether the beneficial owner is a person holding a politically exposed position within the meaning of art. 2 par. 2 item 11) of the Act or has ceased to hold such a politically exposed position within the last 12 months, or is a family member of a person holding a politically exposed position within the meaning of art. 2(3) of the Act or a person who has ceased to hold such a politically exposed position within the last 12 months, or is a person known to be a close associate of a person holding a politically exposed position within the meaning of Article 2(2)(12) of the Act or a person who has ceased to hold such a politically exposed position within the last 12 months,
    b. whether the beneficial owner is a person entered by the General Inspector for Financial Information on the list of persons and entities subject to special restrictive measures referred to in Chapter 10 of the Polish AML Act.
3. A higher risk of money laundering or terrorist financing may be indicated in particular by the fact that:
    a. the ownership structure of the client being a legal entity is not transparent,
    b. the client or beneficial owner is a person holding a politically exposed position within the meaning of Art. 2 sec. 2 item 11) of the Act or has ceased to hold such a politically exposed position in the last 12 months, or is a family member of a person holding a politically exposed position within the meaning of Art. 2(3) of the Act or a person who ceased to hold such a

politically exposed position within the last 12 months, or is a person known to be a close associate of a person holding a politically exposed position within the meaning of Article 2(2)(12) of the Act or a person who ceased to hold such a politically exposed position within the last 12 months,

c. despite taking reasonable actions, Walluta Europe could not establish whether the client or the beneficial owner is a person holding a politically exposed position within the meaning of art. 2 sec. 2 item 11) of the Act or has ceased to hold such a politically exposed position in the last 12 months, or is a family member of a person holding a politically exposed position within the meaning of art. 2(2)(3) of the Act or a person who has ceased to hold such a politically exposed position within the last 12 months, or is a person known to be a close associate of a person who holds a politically exposed position within the meaning of Article 2(2)(12) of the Act or a person who has ceased to hold such a politically exposed position within the last 12 months,

4. A low risk of money laundering or terrorist financing is indicated in particular by the fact that the client is:
   a. a unit of the public finance sector referred to in Article 9 of the Act of 27 August 2009 on public finance (Journal of Laws of 2017, item 2077 and of 2018, item 62),
   b. a company with a majority stake held by the State Treasury, local government units or their associations,
   c. a company whose securities are admitted to trading on a regulated market subject to the requirements of disclosure of information about its beneficial owner arising from the provisions of European Union law or equivalent provisions of law of a third country, or a company with a majority shareholding of such a company.

§ 6

Risk factors concerning countries and geographical areas

1. When identifying the risk of money laundering or terrorist financing and assessing the level of such risk related to the country and geographical areas, Walluta Europe shall take into account, in particular:
   i. the country of residence or registered office of the client,
   ii. country of citizenship of the client,
   iii. country of citizenship of the beneficial owner.
2. A higher risk of money laundering or terrorist financing may be evidenced, in particular, by the fact that:
   i. the country of residence or domicile of the customer, or
   ii. country of citizenship of the customer, or
   iii. the country of citizenship of the beneficial owner,

is:

   i. a high-risk third country referred to in Article 2(2)(13) of the Polish AML Act, as indicated in the statement of the Financial Action Task Force (FATF) published on the website https://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/giif maintained by the GIIF, or

ii. a country with a high level of corruption or other criminal activity, or as a country which finances or supports the commission of acts of a terrorist nature, or with which the activities of organizations of a terrorist nature are associated, or
iii. a country with respect to which the United Nations or the European Union has decided to impose sanctions or specific restrictive measures,

3. A low risk of money laundering or terrorist financing is indicated in particular by the fact that:
   i. the country of residence or domicile of the customer, or
   ii. the country of which the customer is a national, or
   iii. the country of citizenship of the beneficial owner,

is:

i. a Member State of the European Union, a Member State of the European Free Trade Association (EFTA) - a party to the Agreement on the European Economic Area,
ii. a country with a low level of corruption or other criminal activity,
iii. a country which has in force anti-money laundering and anti-terrorist financing regulations corresponding to the requirements arising from the European Union anti-money laundering and anti-terrorist financing regulations.

§ 7

Risk factors regarding the type and subject matter of the transaction

1. When recognizing the risk of money laundering or terrorist financing and assessing the level of the risk associated with the type and subject of the transaction Walluta Europe considers, in particular
   a. the type of virtual currency being the subject of the transaction,
   b. market value of the virtual currency being the subject of the transaction,
   c. form of transaction,
   d. whether the client demand conclusion of the transaction which is non-equivalent on the basis of economic factors,
   e. whether payment by client is made in the amount exceeding 15.000 euro,
   f. whether payment of a pecuniary obligation resulting from the activity included in the notarial deed is funded in significant part with the money obtained from a bank loan or a bank credit,
   g. whether the transaction is carried out in untypical circumstances,
   h. whether transactions of the same property value are performed within a very short time interval,
2. A higher risk of money laundering or terrorist financing may be evidenced in particular by the fact that:
   a. the client demands the conclusion of a transaction which is non-equivalent on the basis of economic factors
   b. payment is made in the amount exceeding EUR 15.000;
   c. the transaction is carried out in untypical circumstances.
3. A low risk of money laundering or terrorist financing is indicated in particular by the fact that:
   a. payment for transaction is financed in a significant part with money obtained from a bank loan or a bank credit,
   b. payment for transaction is financed in full by means of a bank transfer,

c. transaction is concluded due to the occurrence of a legal or economic event which previously caused legal effects for the client.

§ 8

Risk factors balance

1. Walluta Europe, after recognizing the risk factors listed in § 5, 6 and 7 and taking into account the nature of its business as defined in § 2(2), shall assess the risk of money laundering and terrorist financing by applying listed risk factors weighing to determine whether the analyzed transaction is associated with:
    a. a higher risk of money laundering and terrorist financing, or
    b. a medium risk of money laundering and terrorist financing, or
    c. low risk of money laundering and terrorist financing.
2. In accordance with the assessment of the risk of money laundering and terrorist financing Walluta Europe shall apply appropriate financial security measures as specified in the internal procedure on prevention of money laundering and terrorist financing.
3. Determination by Walluta Europe of a higher risk associated with a particular transaction, does not prejudge the fact that there are circumstances that may indicate a suspicion of money laundering or terrorist financing.
4. The weighing of risks shall not lead to circumvention of the provisions of the Polish AML Act or Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing.
5. The result of the application of the risk assessment analysis by Walluta Europe is classification of the client into the appropriate risk group:

    a. Low risk level - group 1
    b. Normal risk level - group 2
    c. High risk level - group 3

§ 9

Final provisions

1. Walluta Europe shall update this risk assessment periodically, at least every 2 years, whenever the risk factors described in this assessment change.
2. In applying this risk assessment, the nature of Walluta Europe as an obliged institution and the provisions of the specification of the business activity in the field of virtual currencies should be taken into account.

§ 10

Risk Matix, latest updated Assessment and Report

The following Risk Assessment and Report with delineating the Risk Matrix, has been conducted inside and by Walluta Europe on 29.12.2023 and the results and findings are still valid at the moment of this latest update of the AML Policy.

ENTERPRISE – WIDE ML/TF RISK ASSESSMENT CONDUCTED ON 29.12.2023 Walluta Europe Sp. z o.o.

Ref	Risk Factors Assessment Questionnaire	Yes/No	Likelihood (ML/TF)	Impact (ML/TF)	Score	Risk Score (Average)/ Risk rating
1.	Any customers who are politically exposed persons?	No	Unlikely	Moderate	2	2.5/Low
2.	Are there customers who are corporate vehicles that are unjustifiably complex, multi-tiered (more than 3 layers)?	No	Unlikely	Moderate	2	
3.	Any customers use nominees' shareholders or shares in bearer form?	No	Unlikely	Moderate	2	
4.	Any customers engaged in higher risk businesses?	No	Unlikely	Major	3	
5.	Has there been negative tax-related news on customers or the jurisdictions where they are from?	No	Unlikely	Major	3	
6.	Any customers requested for hold mail services without satisfactory reasons?	No	Unlikely	Minor	1	
7.	Any customers conducted any suspicious transactions and have been reported to Authorities?	No	Likely	Major	3	

8.	Any customers have been confirmed as a match against sanctions lists and blacklists?	No	Unlikely	Major	3	
9.	Any customer based in or has nationality from a higher-risk country list as determined by FATF or other reliable public sources?	No	Unlikely	Major	3	
10.	Any customers from jurisdictions or countries which are higher risk for tax evasion?	No	Unlikely	Major	3	

Legend

The score for each question is derived using the below table.

		Score		
Impact if ML/TF risk materializes	**Major**	**3**	**6**	**9**
	Moderate	**2**	**4**	**6**
	Minor	**1**	**2**	**3**
		Unlikely	**Likely**	**Very Likely**

Likelihood of ML/TF risk materializing

The likelihood of ML/TF risk materializing and the probability Parameters are assessed as follows:

Likelihood	Probability	% Probability
Very Likely	High likelihood of it happening several times in the next 5 years; or chronic risk with history of occurrence	> 90%
Likely	Could occur more than once in the next 5 years; or can be difficult to control due to some external influences; or has a history of having occurred	16% - 90%
Unlikely	Could occur, but not expected	0% - 15%

The factors considered for an assessment of impact in the event of ML/TF risk materializing are:

Minor	Negligible or minimal consequences or effects;
Moderate	Moderate level of ML/TF impact, inspection report recommending the Company to enhance its AML/CFT policies and procedures; moderate financial loss from regulatory related actions;
Major	Significant level of ML/TF impact, license revocation, reputational loss.

Impact Measurement are assessed as follows:

Consequence Type	Minor	Moderate	Major
Financial Loss	< S$1m	$1m-$10m	> $10m *(Or threatens viability of the company)*
Reputation Loss	Minor isolated stakeholder concerns and impact.	Concerns becoming broader and negative exposure to company	Dramatic loss of stakeholder confidence undermining business viability. Extensive negative public exposure.
Regulatory	Minor regulatory breach and potential review or inspection from regulator.	Moderate implication for business license. Potential regulatory warning and temporary freeze on operations.	Loss of regulatory license. Potential criminal offence and penalties imposed.

The Risk Rating for Customer Risk is derived using the table below:

Range	Rating
=> 6	High
3<=scores<6	Medium
< 3	Low

The inherent risk ratings are interpreted as follows:

Low	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a *low* risk of involvement in ML/TF crimes and a *limited* probability of a ML/TF compliance violation resulting in *limited* exposure to financial or reputation loss arising from a compliance violation.
Medium	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a *moderate* risk of involvement in ML/TF crimes and a *moderate* probability of a ML/TF compliance violation resulting in *moderate* exposure to financial or reputation loss arising from a compliance violation.
High	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a *high* risk of involvement in ML/TF crimes and a *high* probability of ML/TF crimes compliance violation resulting in *high* exposure to financial or reputation loss arising from a compliance violation.

COUNTRY RISK ASSESSMENT

Ref	Risk Factors assessment questionnaire	Yes/No	Likelihood (ML/TF)	Impact (ML/TF)	Score	Risk Score/Risk Rating
1.	Is there evidence of adverse news or public criticism of the country or jurisdiction, including FATF public documents about the country (e.g., the country appears in the FATF list of High Risk and Non-cooperative jurisdictions)?	No	Unlikely	Moderate	2	2/Low
2.	Is there any independent and public assessment of the countries or jurisdiction's overall AML/CFT regime such as FATF or FATF-Styled Regional Bodies' ("FSRBs") Mutual Evaluation reports and the IMF/World Bank Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes for guidance on the countries or jurisdiction's AML/CFT measures?	No	Unlikely	Moderate	2	

3.	Are the AML/CFT laws, regulations, and standards of the country or jurisdiction consistent with those set by FATF?	Yes	Unlikely	Major	3	
4.	Are the implementation standards (including quality and effectiveness of supervision) of the AML/CFT regime such as controls and/or regulation in the country or jurisdiction consistent with those set by FATF?	Yes	Unlikely	Moderate	2	
5.	Is the country or jurisdiction a member of international groups that only admit countries or jurisdictions which meet certain AML/CFT benchmarks?	Yes	Unlikely	Moderate	2	
6.	Are there any contextual factors of concern, such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion, etc.?	No	Unlikely	Low	1	

Legend

The score for each question is derived using the below table.

		Score		
Impact if ML/TF risk materializes	**Major**	3	6	9
	Moderate	2	4	6
	Minor	1	2	3
		Unlikely	**Likely**	**Very Likely**

The Risk Rating for Country Risk is derived using the below table.

Range	Rating
=> 6	High
3<=scores<6	Medium
< 3	Low

The likelihood of ML/TF risk materializing and the probability Parameters are assessed as follows:

Likelihood	Probability	% Probability
Very Likely	High likelihood of it happening several times in the next 5 years; or chronic risk with history of occurrence	> 90%
Likely	Could occur more than once in the next 5 years; or can be difficult to control due to some external influences; or has a history of having occurred	16% - 90%
Unlikely	Could occur, but not expected	0% - 15%

The factors considered for an assessment of impact in the event of ML/TF risk materializing are:

Minor	Negligible or minimal consequences or effects;
Moderate	Moderate level of ML/TF impact, inspection report recommending the Company to enhance its AML/CFT policies and procedures; moderate financial loss from regulatory related actions;
Major	Significant level of ML/TF impact, license revocation, reputational loss.

The inherent risk ratings are interpreted as follows:

Low	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a low risk of involvement in ML/TF crimes and a limited probability of a ML/TF compliance violation resulting in limited exposure to financial or reputation loss arising from a compliance violation.
Medium	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a moderate risk of involvement in ML/TF crimes and a moderate probability of a ML/TF compliance violation resulting in moderate exposure to financial or reputation loss arising from a compliance violation.
High	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a high risk of involvement in ML/TF crimes and a high probability of ML/TF crimes compliance violation resulting in high exposure to financial or reputation loss arising from a compliance violation

PRODUCT/SERVICES/DELIVERY CHANNEL RISK ASSESSMENT

Ref	Risk Factors assessment questionnaire	Yes/No	Likelihood (ML/TF)	Impact (ML/TF)	Score	Risk Score (Average) /Risk Rating
1.	Does the service/delivery channel handle/accept physical cash directly (e.g. over the counter) from to settle any transactions (i.e., cash receipts)?	No	Unlikely	Minor	1	2.6/Low
2.	Does the service involve Virtual Assets?	Yes	Very likely	Major	9	
3.	Does the service allow payment from third parties?	No	Unlikely	Moderate	1	
4.	Does the service allow payment of monies to third parties?	No	Unlikely	Minor	1	
5.	Is non-face-to-face allowed for the establishment of the business?	Yes	Likely	Minor	2	
6.	Is CDD completed before establishing the business relationship?	Yes	Unlikely	Minor	1	

7.	Does the service rely on technology to establish business contacts with clients?	No	Likely	Moderate	2	
8.	Are the Company's products, transactions, and delivery channels particularly susceptible to the following higher risk prevailing crime types? • Corruption • Fraud • Criminal breach of trust • Foreign funding of terrorist activities • Unlicensed moneylending • Unlicensed gaming	No	Unlikely	Major	3	
9.	Is the Company involved in inherently higher risk businesses determined by the National Risk Assessment?	Yes	Likely	Moderate	4	

Legend

The score for each question is derived using the below table.

Impact if ML/TF risk materializes		**Score**		
	Major	**3**	**6**	**9**
	Moderate	**2**	**4**	**6**
	Minor	**1**	**2**	**3**
		Unlikely	**Likely**	**Very Likely**

The Risk Rating for Product/Services/Delivery Channel Risk is derived using the below table:

Range	Rating
=> 6	High
3<= scores < 6	Medium
< 3	Low

The likelihood of ML/TF risk materializing and the probability Parameters are assessed as follows:

Likelihood	Probability	% Probability
Very Likely	High likelihood of it happening several times in the next 5 years; or chronic risk with history of occurrence	> 90%
Likely	Could occur more than once in the next 5 years; or can be difficult to control due to some external influences; or has a history of having occurred	16% - 90%
Unlikely	Could occur, but not expected	0% - 15%

The factors considered for an assessment of impact in the event of ML/TF risk materializing are:

Minor	Negligible or minimal consequences or effects;
Moderate	Moderate level of ML/TF impact, inspection report recommending the Company to enhance its AML/CFT policies and procedures; moderate financial loss from regulatory related actions;
Major	Significant level of ML/TF impact, license revocation, reputational loss.

The inherent risk ratings are interpreted as follows:

Low	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a low risk of involvement in ML/TF crimes and a limited probability of a ML/TF compliance violation resulting in limited exposure to financial or reputation loss arising from a compliance violation.
Medium	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a moderate risk of involvement in ML/TF crimes and a moderate probability of a ML/TF compliance violation resulting in moderate exposure to financial or reputation loss arising from a compliance violation.
High	In the absence of controls, the combination of client, country and services/delivery channel expose the Company to a high risk of involvement in ML/TF crimes and a high probability of ML/TF crimes compliance violation resulting in high exposure to financial or reputation loss arising from a compliance violation.

SUB-TOTAL - Inherent Risk Total Score:

Calculate Inherent risk total score by allocating the relevant risk weightage to each inherent risk factor.

Inherent Risk Factor	Risk Score	Risk weightage	Final Risk Score
Customer Risk	2.5	40%	1
Country Risk	2	20%	0.2
Product/Service/Delivery Channel Risk	2.6	40%	1.04
Total		100%	2.24
Total Risk Rating			**Low**

PART B: ML/TF CONTROL ASSESSMENT

This segment considers the robustness of the Company's Compliance and Control environment:

Areas of Assessment	Controls	Yes/No	Rating	Score	ML/TF Control Score
Governance and Oversight	Is the Company's board of directors and senior management involved in AML/CFT related matters?	Yes	Strong	2	2
	Does the Company have a well-defined reporting structure to the board of directors and senior management on AML/CFT related issues?	Yes	Strong	2	
	Does the Company define the roles and responsibilities of the compliance unit in relation to AML/CFT?	Yes	Strong	2	
	Is there a process of management reporting and escalation of pertinent AML/CFT issues to the Company's senior management?	Yes	Strong	2	
	Does the Company outsource its Head of AML/KYC function?	No	Strong	2	
	Does the Company conduct its own AML/CFT CDD Ongoing Monitoring function?	Yes	Strong	2	
	Is there coordination between AML/CFT compliance and other functions of the Company?	Yes	Strong	2	
	Are the compliance, AML functions, risk management and internal audit staffed by persons with relevant qualifications and experience?	Yes	Strong	2	
	Does the designated AML Compliance Person have sufficient authority within the Company and have adequate resources to fulfil his/her responsibilities?	Yes	Strong	2	
	Does the Company ensure that its AML/CFT policies and procedures are reviewed on a periodic basis?	Yes	Strong	2	
	Does the Company have CDD procedures for its relevant parties ["TRPs"] and/or their effective controllers?	Yes	Strong	2	

Policies and Procedures	Do the Company's AML/CFT policies address the following areas? (a) AML/CFT Roles & Responsibilities of Senior Management and Employees (b) Customer Due Diligence (c) Enhanced Customer Due Diligence (d) ML/TF risk related to Tax Crime (e) Specific risks associated with non- face-to-face contact (f) Ongoing monitoring of Inward/Outward Transactions (g) Periodic review methodology and requirements (h) Suspicious Transactions Reporting Record keeping & documentation standards (j) Training (k) Audit	Yes	Strong	2	2
	Does the Company's AML/CFT policy provide adequate guidance on distinguishing, assessing and corroborating Source of Funds ("SOF") and Source of Wealth ("SOW")?	Yes	Strong	2	
	Does the Company define Politically Exposed Persons and Other High Risk Clients in its AML policy?	Yes	Strong	2	
	Does the Company have specified procedures designed to prevent tipping-off to customer?	Yes	Strong	2	
Audit and Assurance	Does the Company conduct regular audit to ensure that the Company's procedures and the rules and regulations for the prevention of money laundering and terrorism financing are properly implemented and adhered to?	Yes	Strong	2	2
Customer Due Diligence	In the assessment of the Customers, did the Company take into consideration: (a) Customer markets and segments? (b) Countries or jurisdictions customers are from? (c) Volumes and sizes of customers' transactions and funds transfers, considering the usual activities and the risk profiles of customers?	Yes	Strong	2	2

	When performing CDD, does the Company obtain and record all relevant identification and obtained sufficient documents to verify customers?	Yes	Strong	2	
	Does the Company have procedures to identify and verify beneficial owners and all natural persons appointed to act on behalf of customers?	Yes	Strong	2	
	Does the Company have procedure to identify the nature of business?	Yes	Strong	2	
	Does the Company enable account to be opened prior to completing CDD procedures?	No	Strong	2	
	Does the Company have screening procedures in place to check against sanctions and relevant control and alert lists?	Yes	Strong	2	
	Does the Company have procedures in place when relying on intermediaries to conduct CDD on customers?	Yes	Strong	2	
	Does the Company have procedures in place to handle circumstances when it is not able to obtain required identification and verification documents from Customers?	Yes	Strong	2	
	Does the Company have procedures in place to conduct risk assessment and ranks its customers according to risk ratings?	Yes	Strong	2	
	Does the Company have procedures in place to identify source of funds and wealth for high risk customers?	Yes	Strong	2	
	Does the Company have procedures to obtain approval from senior management for onboarding of high risk customers and for escalation of high risk issues?	Yes	Strong	2	

Ongoing Monitoring and Reporting	Does the Company have procedures in place to conduct periodic due diligence checks on customers in accordance to risks assigned?	Yes	Strong	2	2.5
	Does the Company have procedures in place to identify and monitor unusual transactions based on customer risk profile?	Yes	Strong	2	
	Does the Company have procedures to allow non-face-to-face onboarding and are as robust as face-to-face onboarding?	Yes	Average	4	
	Does the Company have procedures in place to document, review and report suspicious transactions?	Yes	Strong	2	
Documenta-tion and Record Keeping	Does the Company maintain records and documentation of Enterprise Risk Assessment?	Yes	Strong	2	2
	Does the Company maintain records and documentation of the CDD process, review of accounts and related transactions, and reports of suspicious transactions?	Yes	Strong	2	
	Does the Company keep records of Declined Business?	Yes	Strong	2	
	In the circumstances when there is complex, unusually large or unusual patterns of transactions, does the Company have specified procedures to document its inquiry into the background and purpose of such transaction(s)?	Yes	Strong	2	

	Does the Company maintain records of any deviation from the Company's AML/CFT policy, e.g. establishing business contacts with TRPs who do not meet the CDD requirements, suspicious transactions that were investigated but subsequently not reported, etc.?	Yes	Strong	2	
Training	Does the Company ensure that staff are adequately informed and trained to be aware of: (a) Their AML/CFT roles and responsibilities in the Company (b) Prevailing techniques, methods and trends in money laundering and terrorism financing (c) Process and procedures for reporting suspicious transactions (d) Process and procedures for handling PEPs, and other high risk customers	Yes	Strong	2	2
	Does the Company conduct regular training/updates on AML/CFT related issues for new and existing staff?	Yes	Strong	2	

Legend

Complete Risk Rating and Score in accordance to the table below:

Rating	Score	Range
Weak	9	=> 6
Average	4	3 < =scores < 6
Strong	2	< 3

Control Weightage

Control Category	Weightage	Rationale
Governance & Oversight	20%	Given highest weighting as effective leadership, communication and monitoring is essential for the efficacy of AML/CFT compliance controls.
Policies and Procedures	15%	A highly important component of AML/CFT program because the existence, maintenance and availability of comprehensive policies and procedures are critical to continued compliance with changing regulatory expectations.
Client Due Diligence	20%	Given highest weighting due to being a crucial prevention control within an AML/CFT program. Additionally, due to the strict regulatory requirements and expectations.
Transaction Monitoring	15%	Highly important as the detection and resolution of potentially suspicious activity is derived from transaction monitoring, investigation and reporting control.
Documentation & Record Keeping	10%	Important to retain institutional knowledge, for continuity, as audit trial of good corporate governance and oversight and act as a protection to employees and the Company.
Training	15%	Highly important that staff are adequately and regularly trained on ML/TF risks and regulatory requirements, policies and procedures and internal controls.
Audit and Assurance	5%	While recognizing the value of independent testing to the framework, it receives the lowest weighting as the absence does not jeopardize the ability of the AML/CFT program to identify potentially suspicious activity through reliance on other controls such as CDD and transaction monitoring.

The control ratings are interpreted as follows:

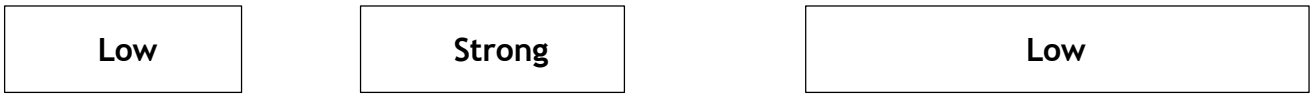
Strong	The control is effective at mitigating inherent risk and there is minimal likelihood of a control breakdown. Risk management practices are highly effective at detecting, remediating, and preventing certain control breakdowns. The control is formally documented and meets or exceeds industry standards, frameworks, and regulatory requirements/guidelines. The control is effective and no audit or critical exam findings have been reported.
Average	A partially effective control indicates that there is some likelihood of a control breakdown. Risk management practices are effective to detect, remediate and prevent certain internal control breakdowns. Testing has identified a moderate number of findings.
Weak	The control is ineffective at mitigating the inherent risk and there is a high likelihood of a control breakdown. Risk management practices are not fully effective to detect, remediate and to a certain extent, prevent internal control breakdowns from occurring. The control is not aligned to industry standards, frameworks, and regulatory requirements/guidelines. Testing has identified a number of critical issues and control weaknesses.

ML/TF Control Total Score

ML/TF Risk Control	Risk Score	Risk weightage	Final Risk Score
Governance and Oversight	2	20%	0.4
Policies and Procedures	2	15%	0.3
Audit and Assurance	2	20%	0.4
Customer Due Diligence	2	20%	0.4
Ongoing Monitoring and Reporting	2	10%	0.2
Documentation and Record Keeping	2	10%	0.2
Training	2	5%	0.1
Total		**100%**	**2**
Total Control Score			**Strong**

Residual Risk = Enterprise-Wide ML/TF Risk

Inherent Risk	-	**ML/TF Controls**	=	**Enterprise-wide ML/TF Risk (Residual Risk)**


Low
Strong
Low

Inherent Risk

Inherent Risk represents the exposure to money laundering, sanctions or bribery and corruption risk in the absence of any control environment being applied. Managing the risk inadequately could lead to reputation risk, regulatory or legal sanction and possible consequent financial costs. Inherent risks are assessed based on client, country and service/delivery channel risks.

Residual Risk:

Residual risks are the risks that remain after controls are applied to the inherent risks. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML/TF risks within the Company are being adequately managed.

Legend

Calculation of Enterprise-wide ML/TF Risk is based on the table below.

Inherent Risk	Control Effectiveness	Residual Risk
High	Strong	Medium
	Average	Medium
	Weak	High
Medium	Strong	Low
	Average	Medium
	Weak	Medium
Low	Strong	Low
	Average	Low
	Weak	Low

ENTERPRISE – WIDE ML/TF RISK ASSESSMENT REPORT

[This report is to be prepared by Compliance, reviewed by Senior Management and approved by Board of Director of Walluta Europe Sp. z o.o.

Company Name	*Walluta Europe* Sp. z o.o.
Date	29.12.2023
Subject	Enterprise-Wide Risk Assessment (EWRA)
Preparer	Werner Wildberger, Member of Management Board
Approver	Werner Wildberger, Member of Management Board

Introduction
Enterprise Wide ML/TF Risk Assessment Report was conducted to assess the overall risk to ML/TF risks to the Company. This is conducted for the company to identify, appraise, manage and supervise risk of ML/TF.
Inherent Risks
Customers: The Company noted that some customers using our services may be of high-risk background. In order to reduce the risk, the Company conducts stringent due diligence checks on all of its customer prior to accepting them as a client. Additionally, the company policy is to refuse services to customers who are PEPs, from negative/ high risk tax jurisdiction or are on sanctions/blacklists. **Country:** Considering that Poland's AML/CFT regulations meets the AML/CFT requirements set by FATF, the country risk is deemed to be low. **Products/Services/Delivery Channels:** Company noted that the product offerings notably virtual assets exchange services is inherently higher risk. In overcoming these, risk, the company have in place measures to mitigate the risk by performing the necessary KYC, CDD and EDD checks prior to accepting any clients. **Overall Inherent Risk:** Overall Inherent risk is considered to be low despite the risk arising out from products/services/delivery channels is medium. This is due to the Customer and Country risk being low as Company tries to minimize and tries to avoid providing Virtual Assets exchange services to high risk customers and only service regulated institutions and corporates.

Controls:
Company has strong overall controls in place, save for its outsourced services where it is deemed average due to the reliance on the service provider have strong controls in place and the company is unable to fully verify these controls. Company will continue to review the controls in place on an ongoing basis to ensure its risk is optimally managed and are in line with regulations.
Residual Risks:
Residual risk is low as the overall inherent risk to Company is low while the ML/TF controls of the Company is strong.
Risk Treatment Action Plans:
Company accepts the inherent risk with its business and continue to monitor such to and risk management procedures to ensure risk of ML/TF is within an acceptable level.
CEO/ Managing Director Comments:
Company's level of risk appetite as a company is at low. Overall risk towards ML/TF is at an acceptable level. Risk management to be assessed continuously.

This Risk Assessment was prepared on 29/12/2023 is effective as of this date.

Werner Wildberger

President of the Management Board / Senior Management representative designated for implementing the duties set out in the Polish Act of March 1, 2018 on counteracting money laundering and financing of terrorism

Signature: