AML POLICY

INTERNAL PROCEDURE FOR COUNTERACTING MONEY LAUNDERING AND TERRORIST FINANCING

KBJ PAY IS THE TRADING NAME OF KBJ SP Z.O.O., REGISTERED IN THE ENTREPRENEURS OF KRS KEPT BY THE DISTRICT COURT KRS: FOR THE CAPITAL CITY OF IN WARSAW, XII COMERCIAL DIVISION OF THE NATIONAL COURT UNDER KRS NUMBER 0000897043 REGISTRATION NUMBER 11650131

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**
08.01.2025	Repeal of the AML Policy dated 20.10.2024 and approval by the Board of Directors of a new Internal Anti-Money Laundering and Terrorist Financing Procedure, dated 08.01.2025, in accordance with Article 50 of the Law on Anti-Money Laundering and Terrorist Financing dated March 1, 2018.	

Definitions:

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

a) AML Reporting Officer – employee, responsible for ensuring the compliance of activity of the obligated institution and its employees and other persons performing activities for the Company 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 (or equivalent if outsourced), 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.

d) the Company - KBJ Pay with its registered seat in Ł ul. Piekna 24/26A, 00-549 Warsaw, Republic of Poland (hereinafter: "the Company"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS Number: 0000897043 Registration number 11650131
e) the Company System/ Software – technological solutions, including software and Customer relationship management, which is use to manage interactions with Customers and potential Customers;
f) Customer (Client) – natural or legal persons, with whom or with which Company is entering into business relationship;
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.
h) 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);
i) Travel Rule - EU Transfer of Funds Regulation no 2015/847 requirements about virtual currency transaction related data collection that are referred to in the Article 58 of the Polish AML Act.

AML Policy content

1. The issue of anti-money laundering and counteracting terrorism has been regulated in:
   a) 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);
   b) 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)
   c) 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)
   d) REGULATION (EU) 2024/1624 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L 2024/1624, 19.6.2024, p.1-111).
2. Money laundering shall be understood as the act referred to in Article 299 of the Act of 6 June 1997
   - Polish Criminal Code, that is:
     Art. 299
     §1. Whoever makes means of payment, financial instruments, securities, foreign exchange values, property rights or other movable or immovable property, originating from the proceeds of the commission of a criminal act, accepts,

possesses, uses, transfers or exports abroad, conceals, transfers or conversion, assists in the transfer of their ownership or possession, or takes other actions that may frustrate or significantly impede the determination of their criminal origin or location, their detection, seizure or ruling of forfeiture, shall be subject to the penalty of deprivation of liberty from 6 months to 8 years.

§2. The penalty specified in § 1 shall be imposed on anyone who, being an employee or acting in the name of or on behalf of a bank, financial or credit institution or other entity which is obligated by law to register transactions and transactors, accepts, in violation of the law, means of payment means, financial instruments, securities, foreign exchange values, performs their transfer or conversion, or accepts them under other circumstances giving rise to a reasonable suspicion that they are the object of an act specified in § 1, or provides other services to conceal their criminal origin or services in securing them from seizure.

§3. (repealed)

§4. (repealed)

§5. If the perpetrator commits the act specified in § 1 or 2, acting in concert with other persons, shall be subject to a penalty of deprivation of liberty for a term of one to ten years.

§6. The punishment specified in § 5 shall be imposed on the perpetrator if, by committing the act specified in § 1 or 2, he or she obtains a substantial financial benefit.

§ 6a. Whoever makes preparations for the offense specified in § 1 or 2, shall be subject to the penalty of deprivation of liberty for up to 3 years.

§7. If convicted of the offense specified in § 1 or 2, the court shall order. Forfeiture of objects derived directly or indirectly from the crime, as well as the proceeds of the offense or their equivalent, even if they are not the they are the property of the perpetrator. The forfeiture shall not be pronounced in whole or in part if the the object, benefit or its equivalent is subject to return to the victim or other entity.

§8. shall not be subject to punishment for the offense specified in § 1 or 2, who voluntarily has disclosed to an authority established for the prosecution of crimes information concerning the persons involved in the commission of the crime and the circumstances of its commission, if this prevented the commission of another crime; if the perpetrator made efforts to disclose such information and circumstances, the court shall apply extraordinary mitigation of punishment.

3. Terrorist financing shall be understood as the act referred to in Article 165a of the Act of 6 June
1997 – Polish Criminal Code; that is:
Art. 165a

§1. Whoever collects, transfers or offers means of payment, financial instruments, securities, foreign exchange values, property rights or other movable or immovable property with the intent to finance a crime of a terrorist nature or an offense referred to in Article 120, Article 121, Article 136, Article 166, Article 167, Article 171, Article 252, Article 255a or Article 259a, shall be punishable by imprisonment from 2 to 15 years.

§2. The same punishment shall be imposed on anyone who makes property specified in § 1 available to an in § 1 to an organized group or association with the purpose of committing an offense referred to in this provision, to a person participating in

such group or association or association or a person who intends to commit such a crime.

§3. Whoever, without being obliged to do so under the law, covers costs related to meeting the needs or fulfilling the financial obligations of the group, association or person referred to in § 2, shall be subject to the penalty of deprivation of liberty for up to 3 years.

§4. The same punishment shall be imposed on the perpetrator of the act specified in § 1 or 2 who acts unintentionally.

4. 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.
5. 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.
6. Financial/non-financial institutions may be misused at any point in the money laundering process.
7. Money laundering shall be regarded as such regardless of whether the exact criminal act from which funds are derived has been identified.
8. 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.
9. 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.
10. 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.
11. The Company 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 the Company 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”.
12. 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.
13. This Policy outlines the minimum general unified standards of internal KYC / AML control which would be adhered to by the Company in order to mitigate the legal, regulatory, reputational, operational, and as a consequence financial risks.
14. The main objectives of this policy are:

a) prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities;
b) enable the Company to know and understand its Customers with which the Company 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 the Company 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 the Company`s personnel with the necessary training and measures to deal with matters concerning KYC/AML procedures and reporting obligations.

15. 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.
16. This Policy is subject to approval by the senior management of the Company. Additionally, this policy is supplemented additionally by various documents which are listed as annexes and templates.

Customer identification – KYC Procedure

17. In order to establish business relation with the Company, Customers have to proceed through specific identity verification procedure (KYC).
18. 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.
19. 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.
20. Customer due diligence comprises a set of activities and practices arising from the organizational and functional structure of the Company and described in internal procedures, which have been approved by the directing bodies of the Company and the implementation of which is subject to control systems established and applied by internal control rules.
21. 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 the Company has reason to suspect money laundering or terrorist financing.

22. 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, the Company 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.
23. 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).
24. Upon establishing a business relationship, the Company 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.
25. 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.
26. The standard Customer Identification Process is CDD. Where the risk associated with a business relationship is low, client is a low risk type and to the extent permitted by national legislation, the Company applies simplified Customer due diligence measures (SDD). Where the risk associated with a business relationship is increased, the Company applies enhanced Customer due diligence measures (EDD). This AML Policy includes provisions for all types of clients, regardless of the scope of services provided in a given period. The scope of clients to whom the services are provided is determined by the resolution of the Board of Directors.

Natural person Customer identification (depends on the Company provided services)

27. To enter into business relation with the Company Customer who is natural person has to provide following data:
    a. Full Name (with first name and last name separation);
    b. Residential Address;
    c. Country of Birth/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 asigned; if not a Polish citizen equivalent of such national number;
    e. Series and number of the document confirming the identity;

f. DOB

28. Customers should submit their identification data and other information (address verification document, information about payment methods) requested by the Company, doing registration process in the Company System, or provide such data to the AML Specialist after AML Specialist requests.
29. 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 KBJ Pay";
    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 KBJ Pay";
    c. driving license - if the name, photograph or facial image, date of birth, citizenship or personal identification code of the holder are entered therein.
30. 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.
31. The Company verifies the correctness of the data specified in this section, using information originating from a credible and independent source for that purpose.
32. The AML Specialist using the personal identity verification and document verification systems (manual or automated or both) provided by the Company 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.
33. After providing of necessary information the Company third party KYC/KYB and AML screening provider makes checks in diverse screening databases, including data present in UN Sanctions Map and Global Watchlist.
34. 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).
35. If the Customer wants to continue collaboration with the Company he/she should to pass full verification process and provide requested documents.
36. The potential or existing Customer shall present identity (personal) documents to the Company:
    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.

37. The Customer's identity (personal) document and other documents submitted to the Company shall satisfy the following requirements:
    a. Identity documents of natural entities shall contain the information listed in clause 27 above;
    b. The documents shall be valid (the validity term specified in the document has not expired at the time of presentation to the Company, 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.);
38. Verification of residence is required by obtaining a copy of an acceptable address proof document issued in the 6 months prior to establishing an business relationship with the Company. 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/ permit.

Business entity Customer identification (depends on the Company provided services)

39. To enter into business relation with the Company Customer who is a legal person (or an organizational unit having no legal personality to whom legal capacity is granted under an legal act) has to provide following data:
    a. the name (business name);
    b. the organizational form;
    c. the address of the registered office (country, city with zip code, street with no of premise)
    d. the Tax Identification Number (for pl: "NIP");
    e. commercial registration number and name of the commercial register
    f. date of registration;
    g. the identification data and measures stipulated in point 12, 13, 14, 15 of the natural person representing entity.
40. The Company 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 and 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.
k. A Certification of Good standing, if in the given jurisdiction such type of document can be provided by the local authorities.

41. The Company verifies that any person purporting to act on behalf of the legal person / entity is properly authorized.
42. 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 the Company.
43. The AML Specialist using the personal identity verification and document verification systems provided by the Company 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.
44. 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 the Company by legal entities with the relevant information about them in the databases.

45. 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.).
46. 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.
47. 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.
48. The AML Specialist verify the data contained in the documents submitted to the Company 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 the Company.
49. 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 Company system.

Identification of Beneficial owner

50. The Company takes measures to identify the beneficial owner(s) of the contractor and verify his identity by obtaining data stipulated in point 27 of this Policy.
51. 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, the Company shall obtain the confirmation of the registration or a copy from the Central Register of Beneficial Owners or the relevant register maintained in a Member State.
52. 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.

53. Identification of the Beneficiary serves the purpose of preventing the provision of services by the Company 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.
54. The AML Specialist shall identify the Beneficiary before establishment of business relations by means of obtaining the minimum information listed in clause 27, in any of the following ways:
    a. Obtaining the information about the Beneficiary of the Customer from the Company system;
    b. Using the data or documents from the information systems of the Republic of Poland or another country, however the Company shall not rely exclusively on the information from the registers 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.
55. 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.
56. 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 the Company about the Beneficiary.

57. Further, guided by considerations of reasonability, proportionality and usefulness on each individual occasion, and where the circumstances mentioned in clause 56 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.
58. If the AML Specialist finds it appropriate, he may:
    a. request the Beneficiary to appear to the Company 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 the Company, such as public databases or the Internet.
59. 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)

60. The Company, as the rule, does not establish (or maintain) business relationship with 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.
61. 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.
62. 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.
63. In order to establish whether a natural person Customer or a beneficial owner is a PEP the Company 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 (EDD)

64. The Company undertakes enhanced financial security measures in the cases of:
    a. higher risk of money laundering or terrorist financing;
    b. (if such type of client will be accepted) business relations with Politically Exposed Persons (PEP), their FM or KCA;
    c. Event- driven actions (transactional monitoring, renewal, etc).
65. 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 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) in Poland (so called 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.

66. 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 27-32 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.
67. In the cases of higher risk of money laundering or terrorist financing the Company verifies also Customer (its representatives and beneficial owner) in sanctions list, in particular:
    a. Warning of The Polish Financial Supervision Authority (KNF);
    b. Warnings of the Polish Office of Competition and Consumer Protection (UOKiK);
    c. United Nations Security Sanction list;
    d. Us Consolidated Sanctions https://www.un.org/securitycouncil/
    e. EU Financial Sanctions https://www.sanctionsmap.eu/#/main, https://eur-lex.europa.eu/, https://eeas.europa.eu/headquarters/headquarters-homepage_en

f. UK Financial Sanctions,
g. Interpol Wanted List,
h. Office of the Superintendent of Financial Institutions (Canada)
i. https://sanctionssearch.ofac.treas.gov/

Monitoring ongoing business relationship

68. The Company 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 the Company 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.
69. The Company 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.
70. 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.
71. 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 the Company system;
    d. Contact with the Customers;
    e. On other affairs specified in the Internal Regulatory Documents.
72. 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.
73. 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.
74. 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 each year;
    b. for the other category risk of Customers – for Medium/Low Risk Customers, every two years;

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.

75. 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.
76. 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.
77. Under checking the Customer data in the Company 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.
78. 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.
79. 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.
80. Under the assessment or opinion on the Customer, the AML Specialist 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.
81. If the AML Specialist 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 category.
82. If the AML Specialist 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.
83. If the Company 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.
84. The Company shall collect from its Customers and provide all necessary data fields required by the GIIF register transaction reporting form, so that the Customer shall provide to the AML Specialist immediately data about transactions over the national threshold (of 15 000 EUR) for their due reporting within up to 7 days as of the date of the transaction.

85. In order to comply with the Travel Rule requirements the Company shall collect KYB and KYC data from its Customers before providing them with VASP services and shall also collect from the transactions made by its Customers all necessary data points required by the Travel Rule. This data shall be transferred to other VASP services providers or competent national or EU authorities upon their request or at least collected and stored by the Company in case of transactions with non-hosted private wallets. The Company shall use blockchain analyze and also KYC/KYB tools and methods of the Company choice to collect data points for the Travel Rule implementation purposes.
86. The Company will designate an employee who will be responsible for collecting and providing to the AML Officer all necessary statistical information data points that required by the GIIF register quarterly statistical reporting form. All the data will be reviewed by AML Officer no later than within 5 working days before the submission deadline of the outstanding quarterly report. Designated employee is responsible for providing AML Officer with all relevant information.
87. The AML Specialist shall prepare the request for information (RFI) including the following data:
    a. The Company 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 the Company;
    d. The Company questions to the Customer;
    e. The manner of the Customer's reply to the request;
    f. The period for replying to the request.
88. The period for replying on the request for submitting the documents and information (the RFI) shall be 7 (seven) working days from the request date.
89. The period specified in clause 88 above may be extended or reduced if the AML Specialist finds it necessary and feasible.
90. If the request for documents and information is prepared, the AML Specialist shall ensure that the term for submitting the documents and information specified in the request is observed. The Customer may submit the documents and information to the Company:
    a. via the Company system;
    b. by e-mail;
    c. in person to the Company employee (if possible).
91. After Customer reply with requested documents and information is received, the AML Specialist shall immediately (within the next following business day) check:
    a. Does the Customer has performed all requirements specified in the RFI, 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.
92. 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.
93. If the Customer does not comply with requirements under request for remove of the identified flaws, the AML Specialist 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.

94. 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.
95. 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 Company 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 the Company 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.
96. 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 AML officer (using the "reply" function via e-mail).
97. 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

98. The AML Specialist should check the ordered and performed transactions of the Customers for detecting suspicious transactions. In case of dubious/ suspicious situation he should address his/her concerns to the AML Officer.
99. In accordance with the AML Policy and Internal Regulatory Documents the AML Specialist should perform the following steps.
    a. Real-time screening;
    b. Retroactive searching;
    c. Transaction monitoring.
    d. 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. the Company system issue a warning to the AML Specialist 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 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 the Company 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 the Company system;
    d. By the AML Specialist using the reporting function in the Company system that allows different report printing in respect of the Customers, transactions or groups of Customers from the Company systems 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 (the CS), 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 the CS 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 Company's 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 the Company system before performing the transaction and as a part of their analysis after the performance. The types of filters, what should be integrated into the Company 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 the Company. Integration of the filters defined by the Member of the Board of the Company into the Company system shall be ensured by the IT department.
111. The filters integrated in the Company 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 the Company system shall be developed by Member of the Board of the Company in cooperation with the IT department and approved by the AML Officer.
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 the Company.

Termination of business relations with the Customer

115. Should the Company 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. The Company terminates 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 the Company 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. The Company 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 the Company or performance of financial transactions) with the Customer and present such draft to the Member of the Board Member of the Company 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 the Company complete data as requested or provide incorrect data or evidently falsified documents, or otherwise attempts to deceive the Company.
c. According to the information available by the Company, 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 the Company 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 the Company abstains from cooperation.
e. The Beneficiary can't provide to the Company additional information by the Company request without important reason.
f. The Company received information from Law Enforcement Agencies that the Customer is subject to any type of financial or asset related criminal proceeding, is wanted, or charged with AML offences/crimes or predicated crimes.

121. Business relations with the Customer shall be terminated based on the decision approved by the Company in accordance with the AML Policy and Internal Regulatory Documents or by the Customer's initiative.

122. The Company have the right to take decision about termination of the business relations approved on the grounds of the Internal Regulatory Documents specifying the following:
a. the Company 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 AML Officer of the Company.

124. Decision about termination of business relations with the Customer shall be implemented as follows:
a. The AML Officer will give approval for termination of business relations with the Customer and block the Customer account in the Company system based on the recommendation by AML Specialist.
b. The AML Officer shall notify all related Employees his/her decision and inform about taken decision via e-mail.
c. The Customer and related persons must be entered into the Company 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 the Company 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 the Company 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 the Company 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 the Company 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 the Company 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 the Company 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. the Company experience from cooperation with the Customer in question;
    e. Other condition that may be relevant for accepting the appropriate decision.

131. The Company 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 or Article 89 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 the Company in relation to the Customer.

b. Electronic versions of the Customer Files at the Company information system including received/executed documents or information in electronic format (such as information tiled in the Company 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. the Company 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 the Company 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. The Company 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 the Company upon processing personal data for AML/CFT purposes is available on the Company webpage in Section Privacy Policy.

138. The Company 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 GIIF 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. The Company shall appoint a person responsible for the performance of the obligations defined in the Polish AML Act.
141. The Company shall appoint the AML Officer – a person, 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 the Company, 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 GIIF of the circumstances which could indicate a suspicion of commission of an offence of money laundering or terrorist financing;
    b. 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.
    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 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 the Company 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. The Company 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 made;
    b. a transfer of funds (incoming, outgoing) 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 144 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. The Company 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 144 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 144 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 the Company;
   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. The Company 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 the Company employee are stipulated in Annex No 1 “Reporting Manual”.

Exclusion of entering business relationship by the Company

150. The Company is not entering into business relations with Customers from a high-risk third country or having a registered office in such a country, unless AML Specialist is able to mitigate the risk. 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

regimes [Search 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 Directive [Search for available translations of the preceding link EN] 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. The Company is not entering into business relations with Customers of UK/US residency.

AML audits

153. The Company is aware that external audits by qualified AML experts provide a needed degree of objectivity in evaluating the internal controls program.

Training

154. As part of the Company Anti- Money Laundering program, all personnel is expected to be fully aware of the Anti- Money Laundering policies. The Company 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.

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. The Company 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 the Company 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. The Company 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 the Company compliance efforts and how to perform them;
    d. the disciplinary consequences (including civil and criminal penalties) for non-compliance.

158. The Company 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 the Company Anti Money Laundering Policy to AML Officer.

Personnel protection

159. The Company 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 [The whistleblowing system].

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 the Company of personal data contained in the reports.

161. The Company 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. The Company 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. The Company 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 the Company exposed to the actions referred to in point 53 shall be entitled to report to the GIIF the instances of such actions.

165. In all other cases not regulated above, the provisions of the AML Act and implementing regulations apply directly.

Law Enforcement Agencies cooperation.

166. In accordance with regulatory standards, the Company's policy outlines specific steps for handling law enforcement queries (the LEQ), ensuring compliance with local and international regulations, and protecting client privacy.

167. Initial Assessment and Classification of LEQ.

a. LEQ Source Verification - upon receiving a law enforcement query, AML Specialist verifies the source of the query.
b. Polish LEQ - queries originating from Polish authorities, such as the police or judiciary, are considered local and should be handled directly.
c. Foreign LEQ - queries from foreign law enforcement authorities must follow the official legal aid channels, in accordance with international legal cooperation protocols.

168. Handling Polish LEQ:

a. Verification of legal validity – AML Specialist must ensure the request from Polish authorities is valid and legally binding (e.g., a court order, warrant, or official directive).
b. If necessary, AML Specialist will consult with AML Officer to ensure the request complies with Polish law.
c. Responding to PL LEQ – AML Specialist provides the requested information or cooperate with the investigation as required by law, first determining the scope of request, than gathering information. If the request is related to any information outside the AML Specialist accesses he/she ask other departments of the company for cooperation.
d. The Response is done by email, and the AML Specialist uses a dedicated mailbox signing information with specially prepared signature "The Compliance Team".
e. The main rule is to follow directly with the scope of request. If sensitive information or transaction details are requested, AML Specialist must ensure that only the authorized data is disclosed.
f. The AML Specialist in dedicated drive creates a folder with Law Enforcement's number of case, where the scan of the request is saved and the printed to pdf response.
g. The AML specialist adds the data regarding the LEQ to the special tracker providing: number of query, date of acceptance in the Company, law enforcement unique number, law enforcement agency which asked, customer name surname, id in the system, mailbox of law enforcement agency to which the response was sent, content of the response, comments if any and AML Specialist name and surname.
h. Any disclosure are documented to maintain compliance with data protection regulations (GDPR).

169. Handling Foreign LEQ.

a. Forward to Legal Aid Channel - queries from foreign law enforcement authorities should not be answered directly. They must be forwarded by the foreign law enforcement agency to the official channels of legal aid, such as the Ministry of Justice or appropriate international bodies.
b. Cooperation with Foreign Authorities - only if required by law, the company should cooperate with international law enforcement but only through the prescribed official channels, ensuring compliance with local and international laws.
c. The AML specialist adds the data regarding the LEQ to the special tracker providing: number of query, date of acceptance in the Company, law enforcement unique number, law enforcement agency which asked, customer name surname, id in the system, mailbox to which information that no action was taken due to incorrect legal proceeding, comment if any and AML Specialist name and surname.

170. Account Blocking Procedure.

a. Criteria for Account Blocking – in each case, when the Company receives LEQ the AML Analyst blocks the Customer's account.
b. Blocking Process – an account is blocked with note added where the number of the case is indicated, no information to the customers is allowed.

171. Periodic Review and Training.

a. Training – the AML Specialist is regularly trained in handling LEQ to ensure he/she understand the Company's policies and procedures.
b. Procedure Review – AML Officer is sampling the tracker periodically, additionally on event-driven basis AML Officer reviews and update procedures to stay compliant with evolving laws and regulations, both locally and internationally.

This AML Policy was prepared on 15.02.2025 is effective as of this date.

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: _____

Name:

Annexes:

1. Annex 1 "Reporting Manual";
2. Annex 2 "Customer Acceptance Policy"
3. Annex 3 "AML KYB Periodic Review Manual (Low, Medium, and High-Risk Clients)"
4. Annex 4 "Third Party Risk Screening Policy"
5. Annex 5 "Internal Travel Rule Policy for VASPs"

Annex No 1 "Reporting Manual"

§1. Introduction

1. 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.
2. 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.
3. KBJ Pay with its registered seat in Ł ul. Piekna 24/26A, 00-549 Warsaw, Republic of Poland (hereinafter: "the Company"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS Number: 0000897043 Registration number 11650131

§2. Internal Suspicious Activity Report (template)

1. When the AML Analyst identifies the suspicious transaction/document/other issue, he/she first prepares an Internal SAR based on the template below.
2. The ISAR is then sent to the AML Officer for review.
3. The AML Officer decides on the next steps, whether the ISAR should be reported to the GIIF (in which case it will become a regular SAR), or whether it should be left without further action.

Part 1 – Involved Parties (*Please create as much tables as needed):

A. Client details /Individual

Name & Surname	
Date of Birth	
Place of Birth	
Nationality	
Address	
E-wallet address	
Contact details	
Additional details	
Description	This section should indicate the involvement of the individual, description how Analyst understand involvement of this party in the activity that is being reported.

B. Client details/ Legal Entity

Section 1:Legal Entity	
Legal Name	
Address	
Company registration number	
Date of establishment	
Country of establishment	
Type of business	
Sort code and account /E-	
Wallet address	
Date account opened	

Section 2: Associated person (UBO)	
Name & Surname	
Date of Birth	
Place of Birth	
Nationality	
Address	
Telephone number	
Email	

C. Other party involved

Name	
Address	
Contact details	
Additional details	Please insert any further details i.e. relevant links
Description	This section should indicate the involvement of the party , description how Analyst understand involvement of this party in the activity that is being reported.

PART 2 Reason for Suspicion

Section 1: Your brief summary of the suspicious activity
Please provide a very brief description…

Section 2: Your description of the reason for suspicion*
In this section, try to answer the following six basic questions to make the information you provide as useful as possible: Who?(all parties involved) What? Where? When? Why? How? Additionally please include: the date of the suspicious activity, type of product or services related how the activity will take place or has taken place when documenting the reason for suspicion. whether the parties involved were successful in opening accounts and carrying out transactions, or whether the system tracked potential fraudsters before they were able to carry out financial operations/purchase transactions. name of the system by which the suspicious activity was detected If you are suspicious because the activity deviates from the normal activity for that individual/firm, briefly explain how the activity that gave rise to your suspicion differs from the normal

*****In this section please try to be as much detailed as possible to make GIIF easier the further proceeding with this SAR.

PART 3 Supporting Evidence

Attach any supporting documentation that is relevant to the case i.e. copies of correspondence, customer files or information you have obtained about the matter, modified documents which have been used etc.

SUSPICION DISCLOSED BY:

SIGNATURE:

POSITION:

DATE:

E-MAIL/PHONE NUMBER:

Received and reviewed by AML Officer:

§3. AML Officer and reporting

1. The AML Officer 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 the Company, that is:
   - information on transactions exceeding threshold limits prescribed in Polish AML Act;
   - notification the GIIF of the circumstances which could indicate a suspicion of commission of an offence of money laundering or terrorist financing;
   - 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;
   - 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;
   - 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 the Company shall justify the reasons for failure to previously provide the notification and provide the information confirming the suspicion.
2. The AML Officer is responsible also for preparing and submitting quarterly statistical report to the GIIF.

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

1. The Company shall provide to the GIIF the information on:
   - a received payment or disbursement of the funds of equivalent in excess of EUR 15,000;
   - transfer of funds exceeding the equivalent of EUR 15,000 from outside the territory of the Republic of Poland;
2. The Company shall provide the information within 7 days from the day of:
   - receipt of the payment or making disbursement of funds - in the case of the information referred to § 3 point (1) subpoint (1);
   - making means of payment available to the recipient - in the case of the information referred to in § 3 point (1) subpoint (1).
3. The counting of the deadline date starts from the day following the event, 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, e.g. if receipt of the payment or making disbursement of funds occurred on 22 January, then the deadline for reporting will expire on 29 January (29 January 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 – in most cases on the Monday.
5. The information shall contain:
   - a unique transaction identifier in the records of the Company;
   - the date or the date and the time of conducting the transaction;
   - the identification data prescribed in § 4 point (6) of the contractor giving an instruction or order of conducting the transaction:
   - available identification data referred to in § 4 point (6) related to other parties of the transaction;

- the amount and currency being the subject of the transaction;
- the transaction type;
- the transaction description;
- method of issuing the instruction or order to perform the transaction;;
- 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:
    i. natural person: name and surname, citizenship, 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, series and number of the document confirming the identity of a person, residence address,
    ii. legal person or an organizational unit without legal personality: name, organizational form, address of the registered office or address of pursuing the activity, 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, identification data referred to in point (5) first subpoint of a person representing such legal person or organizational unit without legal personality.

§5. 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. The Company 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 the Company.
3. The following data shall be provided in the notification:
    a) identification data referred to in § 4 point (6) related to the customer of the Company providing the notification;
    b) available identification data referred to in § 4 point (6) related to natural persons, legal persons or organizational units without legal personality other than customers of the Company;
    c) type and value of assets and place of their storage;
    d) number of the account maintained for the customer of the Company, 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 (6) 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 § 5 point (3) letter (h) the notification to GIIF should, inter alia, contains a justification. This means that the Company, 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).

§6. 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. The Company 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, the Company 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 § 5 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), the Company 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 the Company 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). The Company 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. The Company, 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.

§7. 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. The Company 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, the Company 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 § 7 point (4), in any case no longer than for 96 hours from the moment of submission of the notification referred to in point (1), the Company shall not perform the transaction referred to in § 7 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 § 7 point (3), the prosecutor shall issue the decision on institution or refusal to institute the proceedings, immediately notifying the Company 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 § 7 point (1).
5. The decision concerning the suspension of the transaction or the blocking of the account referred to in § 7 point (4) can be also issued despite the absence of the notification defined in § 7 point (1).
6. In the decision referred to in § 7 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 § 7 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 § 7 point (4) and (7), the Company shall submit, with the use of electronic communication means, information on the notifications referred to in point (1) and copies thereof to the GIIF.

§8. 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. The Company shall immediately notify the GIIF 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, the Company 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 § 6. The provision of § 4 point (5) shall apply accordingly.
2. The Company shall immediately notify the competent prosecutor of performing the transaction referred to in § 7 in the event if the submission of the notification prior to the performance of the transaction was impossible. In the notification, the Company 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 § 7 point (1). The provision of § 7 point (8) shall apply accordingly.

§9. Identification form

1. For the purpose of the first fulfillment of the obligations referred to in § 4, § 5, § 6, § 7 and § 8, the Company shall submit a form identifying the Company to the GIIF.
2. The form identifying the obligated institution contains:
   a) name, including determining of the organisational form of the obligated institution;
   b) NIP;
   c) determining of the type of activity carried out by the obligated institution;
   d) address of the registered office or address of pursuing the activity;
   e) name, surname, position, telephone number and address of electronic mailbox of the AML Officer;
   f) 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 § 9 point (2) the Company shall immediately update them.

§10. Information requested by GIIF

1. On request of the GIIF, the Company 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 § 4 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 the Company took place and times of connections with this system.
2. In the request referred to in § 10 point (1), 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 § 10 point (1) shall be provided and made available free of charge.

Annex No 2 "Customer Acceptance Policy"

KBJ Pay with its registered seat in Ł ul. Piekna 24/26A, 00-549 Warsaw, Republic of Poland (hereinafter: "the Company"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS Number: 0000897043 Registration number 11650131

has set out customer acceptance guidelines as follows:

1. Know Your Customer (KYC) and Customer Due Diligence (CDD) needs to be carried out prior to any Business Relationship or transaction or acceptance of customer transactions.
2. Know Your Customer (KYC) and Customer Due Diligence (CDD) needs to be carried out prior to any Business Relationship or acceptance of customer transactions occasionally.
3. Each Customer, before entering into any Business Relationship or carrying out an Occasional Transaction must pass full verification process. The AML Specialist using the Document Verification System 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;
   c) Document Integrity checks, automatically verification of the authenticity of photos and scaned copies of physical documents check. 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;
   d) Text recognition which allows automatically extract data from the documents;
   e) 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 or duplicated accounts, address check;
   f) Global Watchlist check after all necessary information being provided by relevant software system. The database of a variety of lists across the globe is used 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.
4. Each Customer before entering into Business Relationship with the Company or if he/she wants to continue collaboration with the Company should provide requested documents:
   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.
5. The Customer's identity (personal) document and other documents submitted to the Company shall satisfy the following requirements:
   a) Identity documents of natural entities shall contain the information like: full name (including middle name), residential address, citizenship, number entered in the Polish Universal Electronic System for Civil Registration (PESEL), date and place of birth, series and number of the document confirming the identity;

b) The documents shall be valid (the validity term specified in the document has not expired at the time of presentation to the Company, 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.).

6. 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 the Company. The document must carry the Customer's name and address, if refers to bank statement must carry the sort code and account number. 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;
   g) residence certificate.
7. Before entering into Business Relation with the Company 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 full legal name;
   b) the organizational form;
   c) the address of the registered office and the address of conducting business if differs;
   d) the Tax Identification Number ("NIP");
   e) company registration number;
   f) date of registration;
   g) natural persons acting on behalf of the Customer (UBO, directors, authorized signatories if any) 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.
8. Conducting Enhanced Due Diligence (EDD) for high-risk Customers.
9. 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 the Company undertakes steps to understand the origin and legitimacy of the Customer's wealth and ask Customer for additional documents and information other than stipulated above, 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 Client'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.
10. Senior Management needs to consider and make the final decision to engage in any business relationship or accept customer transactions with high-risk customers.
11. Prohibited Customer means a customer with whom the Company does not establish a Business Relationship or does not carry out Occasional Transactions and includes:

a) persons who have refused to provide required information or documentation, fail to provide sufficient information, fail to provide information regarding their identity, or KYC cannot be conducted;
b) persons who use alias or conceal their true names, or provide false information to conceal themselves;
c) financial institutions that are residents of countries or territories without being physically present in such countries or territories (also referred to as shell banks);
d) correspondent banks that do not have any policies or measures on AML/CTF, or the same fail to comply with global standards or international laws;
e) a person or group of persons or entity that triggers sanctions lists, as announced or provided by AML Officer and international organizations;
f) persons suspected of using the institution as a money laundering channel or using the transactions to finance terrorism and proliferation of weapon of mass destruction financing.

12. Regular and continuous review of Customer information needs to be conducted until a relationship with the customer is terminated.
13. Transaction movements need to be tracked continuously until a relationship with the customer is terminated.
14. Transaction reporting needs to be carried out in accordance with AML/CTF laws. Once suspicious transactions that may constitute money laundering and terrorism financing are detected, AML Officer needs to be notified immediately, for considering further reporting to GIIF.
15. The Customer's risk levels on money laundering and terrorism financing need to be reviewed in accordance with the results of customer information review and customer transaction monitoring.

Annex No 3 "AML KYB Periodic Review Manual (Low, Medium, and High-Risk Customers)"

KBJ Pay with its registered seat in Ł ul. Piekna 24/26A, 00-549 Warsaw, Republic of Poland (hereinafter: "the Company"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS Number: 0000897043 Registration number 11650131

has set out AML KYB Periodic Review Manual (Low, Medium, and High-Risk Customers) as follows:

1. Financial regulators require Virtual Assets Service Providers as obliged institution to perform AML KYB due diligence when onboarding a new Customer and also on a periodic basis throughout the life of the business relationship established with Customer.
2. Purpose of Periodic Reviews:
   a) Regulatory Requirement: Financial regulators mandate AML (KYB) due diligence during customer onboarding and periodically throughout the customer relationship.
   b) Risk Assessment: These reviews ensure that existing Customer's information remains up-to-date and that the assigned risk rating accurately reflects the AML risk.
   c) Detection of Suspicious Activity: Regular reviews help identify any material changes in the customer's profile or potentially suspicious transactions that real-time monitoring might miss.
3. The frequency for performing AML (KYB) reviews shall be conducted, depending on the category or status of the Customer's current risk:
   a) for the High Risk Customers - periodic AML (KYB) reviews should be conducted every 12 months
   b) for the Medium Risk Customers – periodic AML (KYB) reviews should be performed every 24 months
   c) for the Low Risk Customers – periodic AML (KYB) reviews should be performed every 36 months.
4. General key considerations during periodic reviews:
   a) Customer Information: Assess any material changes in name, address, ID number, and other relevant details.
   b) Sanctions Lists: Rescreen against specially designated and country-based sanctions lists
   c) Transaction Analysis: Compare actual transactions with anticipated account activity.
   d) Risk Reassessment: Reapply risk ratings based on any substantive changes in the customer's circumstances
   e) Report Preparation: prepare a periodic review report for the Customer and attach it on the Customer's profile if possible; if not, keep it for future references in a folder dedicated to the Customer.
5. If, after conducting a periodic review for a Customer, it appears that the newly calculated risk is high, the report must be sent to the AML Officer with a request for approval to continue the business relationship with the Customer.
6. After analyzing both, the submitted report together with the supported documentary evidences, the AML Officer may:
   a) approve the continuation of the business relationship with the Customer;
   b) ask for further clarification/documentation from the Customer;
   c) ask for the termination business relationship with the Customer without further investigation, if considers that maintaining a business relationship with a Customer poses too high risk for the Company.

7. If, in the course of conducting a periodic review for a specific Customer, it becomes apparent that the Customer has made a false statement, used a forged or counterfeit document or there are concerns regarding the Customer's transaction activity, indicating that AML Analyst immediately reports the identification of such an event in writing to the AML Officer, who, after analysing the material submitted, will decide on submitting a SAR/STR to the GIIF.
8. In details, when conducting AML (KYB) periodic reviews, the AML Analyst normally review the elements below:
    - review each Customer's information: name, address, ID number, and the customer's original information to determine if there are any material changes;
    - rescreen each Customer's information against various sanctions lists;
    - screen Customers against PEP databases to identify any newly designated individuals;
    - confirm the legitimate Source of funds or wealth for high -risk Customers to mitigate the risk of money laundering;
    - confirm if all documents related the assessed Customer (entity & all individuals) are valid, if not please request valid ones;
    - review the types of transactions performed by each Customer and compare against the forecasted or declared account activity, use automated transaction screening tools as possible and provide a brief summary of received results;
    - determine any potentially suspicious activities that were not detected by the firm's real-time transaction monitoring platforms.
9. To initiate periodic review activities regarding the particular Customer please send via e-mail the following information:

Dear [Customer name],

As part of our ongoing commitment to ensuring the integrity of our services and compliance with regulatory requirements, we are initiating a periodic review of your account.

To facilitate this process, we have attached a template for your completion. Kindly fill out the provided information within 7 working days and return it to us. Your prompt response will greatly assist us in completing the review efficiently.

In the event that we do not receive your completed template within 7 working days, we will follow up with a gentle reminder. Failure to respond within the designated timeframe may result in account termination.

Please be informed that upon receiving completed template from you, we will compare the provided information with your Customer's profile. If any significant changes are noted, we may request additional documents in accordance with our Anti-Money Laundering (AML) Policy.

Thank you for your cooperation in this matter.

Should you have any questions or require further assistance, please do not hesitate to contact us.

Best regards,

[Your Company Name]

and attached the below template to be used to perform Customer's periodic review:

Customer's Periodic Review Template	
Company Name	
Company Trading Name (if different from above)	-
Company website	
Jurisdiction of Incorporation	
Incorporation Date	
Registered Address	
Trading Address (if different from above)	
Is the company regulated?	
What is the company's ownership structure? Please provide.	
Please provide full names, dates of birth & residential addresses of all Directors, Authorised Signatories, Controllers.	
Please provide full names, dates of birth & residential address of all UBOs (25% or more for low & medium Customers, 10% or more for high-risk Customers)	
Please provide full names, dates of birth & residential address of Representative/Agent, if no individual please provide full legal name of the company, date of incorporation, registered address and company registration number.	
Description of SOF /SOW for the business.	
Please provide a brief explanation of the services offered by the business.	
What jurisdictions is the business currently offering services to?	
Name of Submitter	
Position held	
Date	

10. After the Customer sends back the Customer’s Periodic Review Template, the AML Analyst must review the data, compare it with all data available regarding Customer in the Company system and if it appears that the information obtained differs from that on the Customer's profile, update the profile according to the data obtained. In addition, a review of the documents is carried out and if it appears that any documents are missing or no longer valid, the Customer must be asked to provide them.
11. If, in connection with the periodic review, the Customer refuses to submit the form or additional documents requested by the Company, the business relationship with the Customer should be terminated immediately.
12. After each periodic review, all relevant information and findings shall be documented and recorded in the Customer profile (folder). This includes but is not limited to financial data, transaction activity report, customer feedback, and any other pertinent information gathered during the review process. The Customer profile shall serve as a comprehensive record of the Customer's interactions with the organization and shall be updated promptly following each review to ensure accuracy and completeness.

Annex No 4 "Third Party Risk Screening Policy"

1. INTRODUCTION

KBJ Pay with its registered seat in Ł ul. Piekna 24/26A, 00-549 Warsaw, Republic of Poland (hereinafter: "the Company"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS Number: 0000897043 Registration number 11650131

The Company is committed to complying with anti-bribery and corruption laws and regulations, as well as trade sanctions and anti-money laundering regulations implemented by the European Union, particularly Poland as a member state, and any other laws that may apply to the Company's operations in various jurisdictions.

2. OBJECTIVE

Third parties can pose significant legal, operational and reputational challenges to the Company. It is therefore important that the Company always knows who it is doing business with and ensures that its dealings with Third Parties are conducted ethically and in compliance with this Policy and all applicable laws and regulations.

The purpose of this policy is to:

- Establish minimum principles and standards to ensure that the Company complies with: Trade Sanctions Requirements; Anti-Bribery and Corruption Requirements; and- Ethical Business Practices, AML regulations;
- Provide a formal framework for the company's third party due diligence and decision-making process: define the roles and responsibilities of key stakeholders within the company and assess the level of risk posed by each Third Party.
- Mitigate the reputational, operational and legal risks that could arise from a breach of trade sanctions or anti-corruption requirements when dealing with Third Parties.

3. SCOPE

3.1. This policy applies to all business relationships between a Third Party and the Company, whether contractual or otherwise.

3.2. This Policy must be complied with by all employees working for the Company at all levels and grades, including officers, senior managers, directors and employees (whether permanent, fixed term or temporary) wherever they are located.

3.3. The Company also requires that any Third Party working for it who is not an employee of the Company (e.g. consultants, contractors or any other third party acting on behalf of the Company) complies with this Policy.

4. DEFINITIONS

The following terms, whether used in the singular or plural, shall have the following meanings:

Third Party - The term shall be deemed to include similar terms such as vendor, supplier, provider and the like. The term Third Party refers to any person, independent consultant, or form of legal entity, including but not limited to: vendors, service providers, suppliers, processors, business partners, marketers, consultants, agents, or other Third Parties with whom the Company contracts for the purpose of obtaining products or services, or who collaborate with the Company in providing products and services to the marketplace;

Business Requestor - any individual in the Company who wishes to initiate, enter into or renew a relationship with a Third Party. The responsibility for correctly and diligently following the due diligence and approval process rests with the specific individual requesting to initiate, engage or renew the relationship with the Third Party;

Restricted Territories - Countries or territories subject to comprehensive, government-wide or significant sectoral sanctions published by the United Nations Security Council, the European Union, OFAC or the U.S. Department of State, or any other relevant local government authority in the jurisdictions in which the Company operates, including, currently, Cuba, Iran, North Korea, Russia, Syria, Venezuela, the Crimea region and the non-Ukrainian government-controlled areas of the Donetsk, Kherson, Luhansk and Zaporizhzhia regions.

Legal & Compliance Team - the team responsible for onboarding Third Parties, who are required to perform all necessary checks on the Third Party and the information/documents provided by the Third Party in connection with an attempt to establish a business relationship.

5. DECISION MAKING PROCESS - Know Your Business Partner / Customer

5.1. A determination must be made as to whether a counterparty or customer:

1. is of good reputation;
2. raises any red flags for corruption, sanctions or illegal or unacceptable business practices; and
3. has the appropriate business qualifications and expertise for the engagement.

5.2. All Company related third parties within the scope of this policy will be screened against the principal sanctions lists of the European Union, the United States, the United Kingdom and the United Nations, as well as any other lists that may be applicable to the Company's operations in a particular jurisdiction.

5.3. The Company will select Third Parties only on the basis of merit, reputation, integrity and where consistent with the Company's objectives. The Company will NOT enter into a transaction/business activity or continue an existing relationship with a Third Party that is inconsistent with these values and/or is named on a sanctions list or is organised in countries or territories subject to comprehensive sanctions (as defined below, "Restricted Territories").

6. THIRD PARTY SCREENING AND APPROVAL PROCEDURE

Each time a business partner or prospective customer is proposed for a contractual relationship with the Company, the risk-based screening and approval process described in this Policy must be followed:

6.1. Identification: The Business Requestor wishing to engage with a Third Party shall first contact the Legal & Compliance Team ("Compliance") as appropriate.

6.1.1. Third Party does not have an existing contractual relationship with the Company, the Business Requestor must follow the screening and approval process described in this Policy prior to any contractual engagement with the Third Party.

6.1.2. Third Party has an EXISTING CONTRACTUAL RELATIONSHIP with the Company: If the Third Party has an existing contractual relationship with Company and has previously been screened and approved in accordance with this Policy, it is important to confirm whether the prior screening is still valid or whether it has expired due to the passage of time (See section 8 below).

- If the previous due diligence is still valid (according to the validity period in Section 8), the Business Requestor may proceed with the contractual engagement with the Third Party without the need for further screening, subject to changes in the law or other internal business procedures (sourcing, commercial);
- If the previous Due Diligence performed has expired, Business Requestor will need to follow the Due Diligence and approval procedure set out in this Policy prior to entering into any contractual engagement with the Third Party;
- If the third party has previously been vetted and rejected under this procedure, the business applicant must follow the due diligence and approval process set out in this policy.

6.2. Completion and Submission of Due Diligence Questionnaire.

For each relevant Third Party, the Business Requestor will be responsible for completing, or ensuring that the Third Party completes, the External Due Diligence Questionnaire (available in Appendix 1 to this Policy) and then emailing it to Compliance (where available) for review.

6.3. Risk assessment and screening.

Based on the information provided in the External Due Diligence Questionnaire, Compliance will screen the Third Party for sanctions, adverse media and potential PEP engagement using internally available tools (automated and manual) and, based on these results, assign a risk level to the Third Party.

The following risk levels may be assigned to the third party:

Low	• Based in the low or medium risk countries • Low value transaction - no more than [to be determined by the Management Board] annually • No potential conflict of interest disclosed • Low risk sector of activity, no cash involved • No connection with public officials • No adverse media/sanctions match • No red flags in third's party ownership
Medium	• Based in the low or medium risk countries • Low to medium value transaction – from [to be determined by the Management Board] but no more than [to be determined by the Management Board] annually • No potential conflict of interest disclosed • Low to medium risk sector of activity, no cash involved • No connection with public officials

	• No adverse media/sanctions match • No red flags in third's party ownership
High	• Based in the high risk countries, defined as countries included in FATF Grey List and EU High - Risk Countries List • Identified restricted territories or third parties restricted under trade sanctions • High value transaction - over [to be determined by the Management Board] annually • High risk sector of activity, cash payment requested • Potential conflict of interest disclosed • Connection with public officials • Adverse media identified

6.4. Due Diligence and required approvals

The Compliance will verify the information provided in the External Due Diligence Questionnaire and the third-party screening results. According to the Risk Level assigned to the Third Party, they will be categorized as follows.

6.4.1. Low risk Third Parties:

- Low risk Third Parties will be automatically pre-approved - No additional actions and/or Due Diligence required.
- An e-mail confirmation/notification of such approval will be sent by the Compliance to the Business Requestor.

6.4.2. Medium and High risk Third Parties:

- When deemed necessary, the Compliance may conduct additional Due Diligence on the Third Party. This will include, amongst other things, screening of the directors and direct and indirect shareholders.
- Once the verification of available information is completed, the final risk level confirmed, and the potential or existing red flags duly identified, Company will assess whether Company will engage in a business relationship with the Third Party and whether any approval should be conditioned.

Conditions may include:

- Insertion of stricter compliance clauses in the contract (sanctions, ABC, audit, etc.)
- Annual compliance certifications, compliance trainings, etc.
- Monitoring the performance and outcome of the contract.
- Consultation with the Company Management Board.
- An e-mail notification of the final approval or rejection will be sent by the Compliance to the Business Requestor. No approval is valid unless and until such an email is sent. Only after the approval notification is received by the Business Requestor, may contractual engagement with the proposed Third Party proceed in accordance with internal business procedures.

All decisions and documents resulting from the Due Diligence Process, including all the appropriate steps and escalations required to mitigate identified risks, shall be documented both by the Business Requestor and the Compliance.

7. DILIGENCE VALIDITY PERIODS AND RENEWALS

Approved Customers and Business Partners with an existing contract/business relationship with the Company must undergo a refreshed Due Diligence every 2 years for Low & Medium risk Third Parties and at least annually for High risk Third Parties, subject to changes in the law and the application of the Sanctions Policy. Upon expiration, the Business Requestor must renew the due diligence and approval process for the Third Party.

8. MONITORING AND CONTROLS

8.1. Monitoring of the screening process is essential as the Company must be able to satisfy itself that the due diligence process required by law, regulation and/or best practice is being carried out. Each function is responsible for ensuring that any third party it wishes to deal with is screened in accordance with this policy. It is the responsibility of the Business Requestor to ensure that a log is maintained indicating the renewal date of each approval and to renew the request.

8.2. Senior Management shall ensure that the standards and principles in this and all other related policies are implemented and followed by all employees involved in the due diligence process.

8.3. The Compliance Department shall monitor all Third Parties approved to do business with the Company using internally and externally available tools.

8.4. The Business Requestor shall monitor the conduct and performance of its Third Parties during the term of their contracts:

- Appropriate steps shall be taken to identify risks or red flags not previously anticipated or identified;
- Any potential concerns identified must be reported immediately to the Group Legal and Compliance team.

8.5. Periodic review - The operation of this policy will be subject to periodic review to assess the effectiveness of the measures described herein.

9. DOCUMENT RETENTION

The Third Party Business Requestor and Compliance are responsible for maintaining complete, accurate and up-to-date records and supporting documentation related to the screening of Third Parties under this Policy for a period of at least five years.

Annex No 1 : Third Party EXTERNAL DUE DILIGENCE QUESTIONNAIRE

I. GENERAL INFORMATION AND ACTIVITY OF THE THIRD PARTY

Third Party/Company legal name	
Legal status	
Date of creation/incorporation	
Registered Address	
Registered Country	
Ownership structure	
Place and date of incorporation (please provide a copy of the certificate from the applicable commercial register not older than 3 months)	
Stock exchange listed	**YES/NO**
If YES please provide on which one	
What type of services the company offers/performs?	
Sales revenue from last 2 years (please provide the last audited financial statement or tax declaration)	
Please provide the list of countries where the products or services are provided.	
Do you provide any direct/ indirect activities in sanctioned countries/ territories like North Korea, Cuba, Crimea, Donetsk, Kherson, Luhansk, Zaporizhzhya, Russia, Iran, Belarus, Syria, Venezuela?	**YES/NO**
If YES please provide the % of the revenue/ purchases/ investments related to each of such countries/territories .	
Do you provide any direct/ indirect activities with any person listed on any sanctions lists (EU, US, UN or related to other relevant governmental authority e.g. The Specially Designated Nationals).	YES/NO
If YES please provide the % of the revenue/ purchases/ investments related to such persons.	
How the agreement will be documented (contract, invoices only, purchase order, others)	

II. THIRD PARTY BANK ACCOUNT:

Name of the bank	
Bank address	
Account number	
Account holder name	
How payment will be made?	

III. RELATIONSHIPS WITH PUBLIC OFFICIALS

Are you a public third party?	**YES/NO**
If YES indicate which % of shares is held by the public official or the public entity	
Are PEP involved in your organization (shareholder, director, manager, controller, UBO) ?	**YES/NO**
If YES please provide the full name of the public function he/she was entrusted with.	

IV. DIRECTORS /MANAGERS

Position	**Full Name**	**Nationality/Residence**	**Date of Birth**
President			
CEO			
CFO			
CCO			
COO			

V. AUTHORIZED PERSON* (for each individual please provide Proof of Identity and Proof of Address)

Position	**Full Name**	**Nationality/ Residence**	**Date of Birth**	**Residential Address**

*Third Party's authorised representative for contacts with the Company

VI. DIRECT SHALHOLDERS/ ULTIMATE BENEFICIALS OWNERS* (individuals or entities which owns directly or indirectly 25% or more of shares or having the controlling power over THIRD PARTY)

Position	**Full Name**	**Country of Incorporation** (if entity)	**Nationality /Residence** (if individual)	**Residential address**

*(for each individual please provide Proof of Identity and Proof of Address, if legal entity involved please provide the extract from the relevant commercial register and POA. Please be advised that the Company may ask for further supporting evidences as necessary.)

VII. REPUTATIONAL RISK RELATED TO THIRD PARTY

Please describe if there have been any situations in the past in connection with which the company was fined, if YES please briefly describe what the situation concerned	

VIII. CONFLICT OF INTEREST DISCLOSURE

To the best of your knowledge does any conflict of interest exist between your company, shareholders, authorized persons, directors, any other employee?	
Any Company director, officer or employee? Please describe if YES	**YES/NO**
Any potential or current customer of the Company ? Please describe if YES	**YES/NO**

IX. COMPLIANCE & ETHICS

Do you have any Whistleblowing Policy? **If YES please attach copy.**	**YES/NO**
Do you have any Anti – _Corruption and Bribery Policy? **If YES please attach copy.**	**YES/NO**
Do you have and AML/KYC Policy or any Compliance Program? **If YES please attach copy.** **If NO please provide explanation.**	**YES/NO**
Do you have any Sanctions Policy ? **If YES please attach copy.**	**YES/NO**
Do you have Code of Conduct or any other similar document ? **If YES please attach copy.**	**YES/NO**
Are there any red flags in relation to this potential business relationship that Company should be aware of. **If YES please provide more details.**	**YES/NO**

By submitting this Questionnaire, the representative of the Third Party warrants that the information provided here-in is accurate and complete at the date of submission.

Date: _____

Signature: _____

Annex No 5 "Internal Travel Rule Policy for VASPs"

1. Introduction

This policy establishes detailed procedures and measures for Virtual Asset Service Providers (VASPs), which is compliant with EU terminology of Virtual-Asset Providers (VASPs) to comply with Regulation (EU) 2023/1113[1]. This regulation extends the scope of the "travel rule" to include virtual asset transfers, aiming to enhance the traceability of transactions to combat money laundering (ML) and terrorism financing (TF). It outlines the necessary steps VASPs must take to detect, manage, and transmit required information for transfers.

2. Definitions

(1) 'payer' means a person that holds a payment account and allows a transfer of funds from that payment account or, where there is no payment account, that gives a transfer of funds order;

(2) 'payee' means a person that is the intended recipient of the transfer of funds;

(3) 'payment service provider' means the categories of payment service provider referred to in Article 1(1) of Directive (EU) 2015/2366[2], natural or legal persons benefiting from a waiver pursuant to Article 32 thereof and legal persons benefiting from a waiver pursuant to Article 9 of Directive 2009/110/EC[3], providing transfer of funds services;

(4) 'intermediary payment service provider' means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee or of another intermediary payment service provider;

(5) 'payment account' means a payment account as defined in Article 4, point (12), of Directive (EU) 2015/2366[4];

(6) 'funds' means funds as defined in Article 4, point (25), of Directive (EU) 2015/2366[5];

(7) 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:

   i. a credit transfer as defined in Article 4, point (24), of Directive (EU) 2015/2366[6];
   ii. a direct debit as defined in Article 4, point (23), of Directive (EU) 2015/2366[7];
   iii. a money remittance as defined in Article 4, point (22), of Directive (EU) 2015/2366[8], whether national or cross-border;
   iv. a transfer carried out using a payment card, an electronic money instrument, a mobile phone or any other digital or IT prepaid or postpaid device with similar characteristics;

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1113

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0110

[4] Please see (2)

[5] Please see (2)

[6] Please see (2)

[7] Please see (2)

[8] Please see (2)

(8) ‘transfer of virtual-assets’ means any transaction with the aim of moving virtual-assets from one distributed ledger address, virtual-asset account or other device allowing the storage of virtual-assets to another, carried out by at least one virtual-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the virtual-asset service provider of the originator and that of the beneficiary are one and the same;

(9) ‘batch file transfer’ means a bundle of several individual transfers of funds or transfers of virtual-assets put together for transmission;

(10) ‘unique transaction identifier’ means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, or determined by a virtual-asset service provider, which permits the traceability of the transaction back to the payer and the payee or the traceability of the transfer of virtual-assets back to the originator and the beneficiary;

(11) ‘person-to-person transfer of virtual-assets’ means a transfer of virtual-assets without the involvement of any virtual-asset service provider;

(12) ‘virtual-asset’ means a virtual-asset as defined in Article 3(1), point (5), of Regulation (EU) 2023/1114[9], except where falling within the categories listed in Article 2(2), (3) and (4) of that Regulation or otherwise qualifying as funds;

(13) ‘virtual-asset service provider’ means a virtual-asset service provider as defined in Article 3(1), point (15), of Regulation (EU) 2023/1114[10], where performing one or more virtual-asset services as defined in Article 3(1), point (16), of that Regulation;

(14) ‘intermediary virtual-asset service provider’ means a virtual-asset service provider that is not the virtual-asset service provider of the originator or of the beneficiary and that receives and transmits a transfer of virtual-assets on behalf of the virtual-asset service provider of the originator or of the beneficiary, or of another intermediary virtual-asset service provider;

(15) ‘virtual-asset automated teller machines’ or ‘virtual-ATMs’ means physical or on-line electronic terminals that enable a virtual-asset service provider to perform, in particular, the activity of transfer services for virtual-assets, as referred to n Article 3(1), point (16)(j), of Regulation (EU) 2023/1114[11];

(16) ‘distributed ledger address’ means an alphanumeric code that identifies an address on a network using distributed ledger technology (DLT) or similar technology where virtual-assets can be sent or received;

(17) ‘virtual-asset account’ means an account held by a virtual-asset service provider in the name of one or more natural or legal persons and that can be used for the execution of transfers of virtual-assets;

(18) ‘self-hosted address’ means a distributed ledger address not linked to either of the following:

i. a virtual-asset service provider;

ii. an entity not established in the Union and providing services similar to those of a virtual-asset service provider;

[9] https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[10] Please see (9)

[11] Please see (9)

(19)'originator' means a person that holds a virtual-asset account with a virtual-asset service provider, a distributed ledger address or a device allowing the storage of virtual-assets, and allows a transfer of virtual-assets from that account, distributed ledger address, or device, or, where there is no such account, distributed ledger address, or device, a person that orders or initiates a transfer of virtual-assets;

(20)'beneficiary' means a person that is the intended recipient of the transfer of virtual-assets;

(21)'legal entity identifier' or 'LEI' means a unique alphanumeric reference code based on the ISO 17442 [12]standard assigned to a legal entity;

(22) 'distributed ledger technology' or 'DLT' means distributed ledger technology as defined in Article 3(1), point (1), of Regulation (EU) 2023/1114[13].

3. Scope and Applicability.

This policy applies to all virtual asset transfers processed by the company, covering:

i. VASPs handling the originator or beneficiary data,
ii. Intermediary VASPs (IVASPs [ICASPs]) managing transmission within the transfer chain.

4. Information Requirements.

All virtual-asset transfers must include information[14]:

i. Originator Details:
   a) Full name,
   b) wallet identifier or equivalent,
   c) address, or unique personal identifier.
ii. Beneficiary Details:
   a) Full name
   b) wallet identifier or equivalent.

5. Procedures for Missing or Incomplete Information.

VASPs must implement stringent procedures to identify and address missing or incomplete data:

i. Initial Detection – implementation of the monitoring systems to flag transfers with missing, nonsensical, or incomplete information.
ii. Risk-Based Review – assessment of flagged transfers according to the level of ML/TF risk.
iii. Corrective Measures - notify the originating VASP or intermediary for required data. Deadlines for data provision are as follows: three days for intra-EU transfers, five days for non-EU transfers.

6. Handling Self-Hosted Wallets.

Transfers involving self-hosted wallets require specific measures:

i. Verification – mandatory confirmation of the ownership or the control of self-hosted wallet addresses for transfers exceeding EUR 1,000 [after MiCA enters into force EUR 1,0].

[12] https://www.iso.org/standard/75998.html

[13] Please see (9)

[14] as stipulated by Articles 4, 7, 11, and 14 of Regulation (EU) 2023/1113

ii. Identification - blockchain analytics, customer data, and verification tools usage for assurance for accurate identification of parties involved.
iii. Revision – review of all customer-submitted documents and utilize third-party verification services to supplement verification efforts when necessary.
iv. High Risk Jurisdiction wallets - enhanced scrutiny should be applied when self-hosted wallets are linked to high-risk jurisdictions.

7. Technical Infrastructure and Data Integrity.

Data integrity is maintained throughout the transfer process:

i. Data Transmission Security - VASPs must use secure, encrypted channels to maintain the confidentiality and integrity of transfer data.
ii. Data Conversion – a conversion of data formats must preserve the completeness and accuracy of transmitted information.
iii. System Capabilities – the systems must be secure, interoperable, and capable of transmitting complete data.

8. Non-Compliant Transfers.

VASPs manage non-compliant transfers through the following:

i. Suspension or Rejection - transfers may be suspended or rejected if essential data is not provided despite follow-up.
ii. Recurrent Non-Compliance - VASPs must report and monitor transfers from other VASPs known for repeated failures to provide required information.
   - Identification and documentation recurring non-compliance from other VASPs or IVASPs.
   - Reporting such type of cases to competent authorities, ensuring that thorough records are kept.
iii. Format Preservation - if data format conversion is required, the original information must remain intact, ensuring no data corruption or loss occurs during processing.
iv. Mitigation Strategies - VASPs should maintain a risk-based approach in deciding future business with repeatedly non-compliant entities.

9. Record-Keeping and Reporting.

Maintain comprehensive records of transfer data and flagged transactions. Reports on non-compliant VASPs must be submitted to competent authorities no later than three months after identifying repeated failures.

i. Data Logs – it is mandatory to keep detailed logs of all transfer data and monitoring activities, especially transactions flagged for incomplete information.
ii. Regulatory Reporting – each non-compliant VASPs should be reported to the relevant authorities within three months of identifying repeated failures.
iii. Review Mechanisms: Implement regular audits to ensure that record-keeping practices align with regulatory standards.

10. **Monitoring and Review.**

Regularly review and update the policy to ensure alignment with current regulations and best practices.

i. Compliance Audits - periodic audits must be conducted to verify adherence to this policy.
ii. Policy Updates - timely updates to be prepared to incorporate any changes in regulations or operational practices.

11. **Staff Training and Compliance**

Ensure all relevant employees are trained on compliance requirements. Internal audits should be conducted to verify adherence to these procedures.

i. Mandatory Training - all employees involved in handling virtual asset transfers must undergo training on regulatory compliance and the operational procedures outlined in this policy.
ii. Compliance Checks - regular checks and assessments should be performed to ensure that staff understand and adhere to these procedures.
iii. Feedback Loop – constantly opened channel to collect feedback from employees to improve training programs and procedural clarity.

Effective Date:

This policy takes effect on 08 January 2025.