

Policy of Tiwala Solutions Korlátolt Felelősségű Társaság on measures taken for the prevention and combating money laundering and terrorist financing

Valid from 01 November 2022 until withdrawal

Table of contents

I. PURPOSE OF THE POLICY	3
II. PERSONAL AND MATERIAL SCOPE OF THE POLICY	3
III. RELATING LEGISLATIONS	3
IV. EXPLANATORY NOTES	3
V. CUSTOMER DUE DILIGENCE DUTY AND IMPLEMENTATION OF MEASURES	6
V.1. The customer due diligence duty	6
V.2. Interim measures	7
- checking of the client's identity based on the client's personal data, documents suitable for verifying personal data provided as specified in paragraph V.3.3, as well as providing e-mail address and telephone number, in person or electronically, via the Service Provider's website,	7
- completion of client identification data sheet, the politically exposed person declaration and, in the case of non-natural person (organizational) clients, the beneficial owner Declaration among the forms specified in the annexes to this Policy.	7
V.3. Customer due diligence measures	7
As part of the customer due diligence, the Service Provider implements the following measures:	7
i. identification of the client, recording of personal data,	7
ii. the risk rating of the client (in writing in case of possible establishment of a long-term business relationship),	7
iii. verification of identity, validity and authenticity check with regard to the documents that have been presented by the client, the assignee thereof, the authorized representatives, and proceeding representative thereof,	7
iv. learning and continuous monitoring of the business relationship and the purpose and characteristic of the transaction order, conduction of enhanced procedure (in cases specified in the Policy)	7
v. identification of the beneficial owners of the organizational client, declaration regarding the status of the beneficial owners as politically exposed persons,	7
vi. Query from the beneficial ownership register	7
vii. Difference signal	7
viii. recording of data on the source of the funds involved in the transaction relationship, examination of the documents submitted to verify the data;	7
ix. if necessary, the verification of the source of funds involved in the business relationship and the examination of the documents submitted for verification.	7
V.3.1. Identification and verification of identity	7
V.3.2. Identification of the order	8
V.3.3. Documents to be submitted	9
V.3.4. Procedure of representatives	10
V.3.5. Identification of beneficial owners	10
V.3.5.1 – Specification of the beneficial owner and recognition of complex ownership structures	11
V.3.5.2. Query from the register of beneficial owners and difference signal	11
V.3.6. Politically exposed person status	11
V.3.7. Other rules	11
V.3.10. Cases of termination of business relationship	12
V.4. Simplified customer due diligence (SDD)	12
V.5. Enhanced customer due diligence (EDD)	13
V.5.1. Client personally not appearing	13
V.6. Customer due diligence carried out by other service provider	13
VI. IMPLEMENTATION OF FINANCIAL AND ASSET RELATED RESTRICTIVE MEASURES (SANCTION AND EMBARGO)	14
VII. DATA PROTECTION, REGISTRATION	14

I. PURPOSE OF THE POLICY

A service provider providing exchange services between virtual and legal tender and virtual currencies shall be obliged to implement an internal policy as a result of the amendment to the Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter referred to as **AML Act**).

In view of the above obligation, **Tiwala Solutions Korlátolt Felelősségű Társaság** (registered office: 1131 Budapest, Mosoly u. 40 / A 1st floor, company registration number: 01-09-343101, tax number: 26757489-2-41, hereinafter: "**Service Provider**"), as a supervised entity subjected to anti-money laundering and terrorism financing regulations, adopted its internal AML policy (hereinafter: **Policy**) to consolidate and to provide a standardized regulation of the tasks, activities to be carried out and procedures to be followed. The aim of this published document is to highlight prescriptions as to the duties of clients and the procedure of the Services Provider regarding the clients.

The Service Provider proceeds risk based, it identifies, assesses its anti-money laundering and terrorism financing risks linked to its operation (customers, product/services, geographical extension, transactions channels) and in view of these defines the measures aiming the prevention and management of these risks and the absolutely excluded client relationships.

II. PERSONAL AND MATERIAL SCOPE OF THE POLICY

The personal scope of the Policy shall cover all clients of the Service Provider, the person authorized to dispose on behalf thereof, assignees and representatives thereof, as well as all organizational units and workers, representatives, employees, staffs and agents, assignees and cooperating partners assigned for the fulfilment of the obligations specified in this Policy.

The material scope of the Policy shall cover the activities performed by the Service Provider during the exchange of virtual and legal tender instruments and virtual payment instruments for the prevention and combating of money laundering and terrorist activities, such as risk rating, due diligence and monitoring of clients, the implementation of duties related to the reporting and registering of suspicious transactions and circumstances, the suspension of transactions, and furthermore for the implementation of financial and asset restrictive measures.

III. RELATING LEGISLATIONS

Relating legislations:

- AML Act,
- Act C of 2012 on the Criminal Code (hereinafter: the Criminal Code), and the Act IV of 1978 (hereinafter: the old Criminal Code),
- Act V of 2013 on the Civil Code (hereinafter: the Civil Code), and the Act IV of 1959,
- Act LIII of 1994 on the law on judicial enforcement,
- Governmental Decree No. 485/2015 (XII.29.) on the jurisdiction and competence of the National Tax and Custom Administration bodies,
- Act XC of 2017 on Criminal Proceeding, and the Act XIX 1998,
- Act LII of 2017 on the enforcement of financial and asset related restrictive measures ordered by the European Union and the Security Council of the UN („Kit”),
- Act LIII of 2017 on the prevention and combating of money laundering and terrorism financing and Ministry of National Economy Decree No. 21/2017 (VIII.3.) on the contents of the internal policy to be prepared upon the Act LII of 2017 on the financial and asset related restrictive measures ordered by the European Union and the Security Council of the UN (hereinafter NGM Decree)
- 2/2021. (II.2.) Ministerial Decree of Ministry of Finance on the detailed rules for the implementation of the AML Act and the minimum requirements for the development and operation of a filtering system according to the Public Administration Act for certain non-financial service providers covered by the legislation on the prevention and prevention of money laundering and the financing of terrorism (hereinafter the Minister of Finance Decree).

IV. EXPLANATORY NOTES

Under this policy:

1. **audited electronic means of communication:** audited electronic system that allows distance customer due diligence via an electronic data transmission channel, the issuance, interpretation, secure storage of the client statements, retrieval and monitoring of stored data,
2. **identification:** record of data specified in paragraph 7(2), 8(2) and (3), and 9(1) and (2) of the AML Act, in a traceable manner,
3. **electronic client identification system:** such personalized electronic procedure that allows the issuance of declarations in a form that clearly identifies the declarant and the date of the declaration and the retrieval of the unchanged content of the declaration,
4. **dominant influence:** the decisive influence under the definition of a parent company under Act C of 2000 on Accounting (hereinafter: the Accounting Act) or the relationship between a person and an undertaking on the basis of which
 - a) the influential person may decide on the distribution of the undertaking's profits, the transfer of its profits or losses to another undertaking, its strategy, its business policy or its sales policy,
 - b) whether the agreement is established in the statutes (articles of association) or in another written contract, the alignment of the undertaking's management with another undertaking's management is possible for a common purpose,
 - c) joint control is exercised by partly (but representing a majority of the decisions required) or entirely identical composition of the management or supervisory board of the undertakings, or
 - d) the influential person exercises significant influence over the operation of another undertaking without a capital injection,
5. **Difference signal:** an institutionalized indication on data providers, namely the beneficial owners of the Service Provider's clients included in the beneficial ownership register, related to some data registered thereabout, and reflecting an inaccuracy according to the person making the notification, on the basis of which a duty is being established both on the registration authority's and the data provider's side.
6. **European Union:** the European Union and the European Economic Area,
7. **Member State of the European Union:** Member State of the European Union and other country party to the Agreement on the European Economic Area,
8. **Resolution of the United Nation's Security Council:** the resolution adopted by the UN Security Council for the maintenance of international peace and security, as defined in Article 25 of the Charter of the United Nations, promulgated by Law I of 1956,
9. **FIU:** the authority acting as the Financial Intelligence Unit in relation to the provisions of the AML Act, the body responsible for taking the financial and asset related restrictive measure in relation to the provisions of the Kit,
10. **third country:** any state that is not a member of the European Union,
11. **certified translation:** translation prepared by the Hungarian Office for Translation and Attestation,
12. **official translation:** proofread, stamped, concatenated and attested translation, whereby an official clause verifies that the completed translation corresponds to the text delivered to the translation office.
13. **unincorporated organization:** any legal entity other than legal persons and natural persons,
14. **politically exposed person:** a natural person who is entrusted with prominent public functions, or who has been entrusted with prominent public functions within one year before the implementation of customer due diligence measures.
15. **natural person with prominent public functions shall include:**
 - a) heads of State, heads of government, ministers and deputy ministers, state secretaries, in Hungary the head of State, the Prime Minister, ministers and state secretaries,
 - b) members of parliament or of similar legislative bodies, in Hungary members of parliament and spokesmen for the nationality,
 - c) members of the governing bodies of political parties, in Hungary members and officers 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, in Hungary members of the Constitutional Court, of the courts of appeal and the Curia,
 - e) members of courts of auditors or of the boards of central banks, in Hungary the President and Vice-President of the State Audit Office, members of the Monetary Council and the Financial Stability Board,
 - f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces, in Hungary the head of the central body of law enforcement bodies and organizations and his deputy, Chief of Staff of the Hungarian Army and Deputy Chiefs of Staff of the Hungarian Army,

- g) members of the administrative, management or supervisory bodies of undertakings with majority state ownership, in Hungary the managing directors of undertakings with a state ownership, including members of the management body exercising control or supervisory rights of such undertakings,
 - h) directors, deputy directors and members of the board or equivalent function of an international organization.
16. **family members of politically exposed person:** the spouse or domestic partner of a politically exposed person; the biological and adopted children, stepchildren and foster children and their spouses or domestic partners, of a politically exposed person; the biological, adoptive, step- and foster parents of a politically exposed person.
 17. **close associates of politically exposed persons:**
 - a) any natural person who is known to have joint beneficial ownership of legal entities or unincorporated organizations, or any other close business relations, with a politically exposed person,
 - b) any natural person who has sole beneficial ownership of a legal entity or unincorporated organization which is known to have been set up for the benefit of a political exposed person
 18. **risk sensitivity approach (risk based approach):** a procedure specified in an internal policy relying on the outcome of internal risk assessment, based on the nature and value of the business relationship or the transaction order, and on the client's circumstances, for the purpose of prevention and combating money laundering and terrorist financing;
 19. **enhanced procedure:** an enhanced monitoring including risk-based measures for the management of the risk inherent in the client, the product, the service, the transaction, the applied asset or the geographical exposure,
 20. **monitoring:** continuous follow-up of the business relationship,
 21. **verification of source of funds:** information confirming the legal source of the funds involved in the transaction or a document providing a certification thereon, such as in particular a contract of inheritance, compensation, civil law relationship or other official document specifying the attached entitlements, proof of income from employment, proof of income from external service, other income certificate, documentary evidence related to foreign exchange gains, prize, dividends
 22. **money laundering:** conducts defined in section 303-303/A of the old Criminal Code, and in section 399-400 of the Criminal Code,
 23. **money laundering and terrorism financing risk:** possibility and effect of the likelihood of money laundering and terrorism financing,
 24. **national financial intelligence unit:** a department of the National Tax and Customs Authority delegated by the relevant legislation (FIU),
 25. **financial and asset related restrictive measures:**
 - a) freezing of financial and asset funds ordered by Union acts, or the UN SC resolution,
 - b) restriction on making financial and asset funds available ordered by Union acts, or the UN SC resolution, and
 - c) restriction, limitation, and relating authorization procedure ordered with regard to financial transactions (transfer of funds) specified by the Union act, or the UN SC resolution,
 26. **subject of the financial and asset related restrictive measure:** natural or legal person, unincorporated organization under the Union act, or the UN SC resolution ordering financial and asset related restrictive measure, and the natural or legal person, unincorporated organization that is the member of the organization under the Union act, or UN SC resolution ordering financial and asset related restrictive measure,
 27. **high-risk third countries with strategic deficiencies:** the countries provided for in Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies
The list of high risk third countries with strategic deficiencies for current and previous periods is available at the following link:
<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A02016R1675-20220313&qid=1654077645736>
 28. **official document suitable for identification purposes:** a personal identity card, passport, and driving license in card format,
 29. **verification of identity:** the procedure to verify the identity of the client, agent, proxy or other authorized representative, and to check the identity of the beneficial owner,
 30. **effectively connected, multiple business orders:**
 - a. those transactions for which the same client gives an order within one year under the same legal title and on the same subject,

- b. in case of the currency exchange office, those transactions for which the same client gives an order within one week,
 - c. payments based on instalments, payment orders in relation to commodity dealers.
- 31. **beneficial owner:**
 - a) any natural person who owns or controls at least twenty-five per cent of the shares or voting rights in a legal person or an unincorporated organization directly or - by way of the means defined in paragraph 8:2(4) of Act V of 2013 on the Civil Code - indirectly, or who is able to exercise effective control over the legal person or unincorporated organization via other means, if that legal person or unincorporated organization is not listed on a regulated market and is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards,
 - b) any natural person who has a dominant influence in a legal person or unincorporated business association as defined in paragraph 8:2(2) of the Civil Code,
 - c) any natural person on whose behalf a transaction is being conducted, or who is able to exercise effective control over the activity of a client via other means in the case of natural persons,
 - d) in the case of foundations:
 - i. where the future beneficiaries have already been determined, the natural person who is the beneficiary of twenty-five per cent or more of the property of the foundation,
 - ii. where the individuals that benefit from the foundation have yet to be determined, the natural person in the interest of whom the foundation is set up or operates, or
 - iii. the natural person who exercises control in the management of the foundation or exercises control over at least twenty-five per cent of the property of a foundation, and/or who is authorized to represent the foundation,
 - e) in the case of fiduciary asset management contracts:
 - i. the principal, and the beneficial owner referred to in point a) or b) thereof,
 - ii. the fiduciary, and the beneficial owner referred to in point a) or b) thereof,
 - iii. the beneficiaries or class of beneficiaries, and the beneficial owner referred to in point a) or b) thereof in case of persons other than a natural person beneficiary, furthermore
 - iv. the natural person who otherwise exercises control over the managed assets,
 - v. auditors of fiduciary asset management
 - vi. any natural person exercising effective control over the trust fund via other means, furthermore
 - f) in the absence of the natural person referred to in points a) and b), the executive officer of the legal person or unincorporated business association,
- 32. **Union legal acts:** Union acts adopted on the basis of Articles 75 and 215 of the Treaty on the Functioning of the European Union, and acts or measures adopted on the basis of those acts,
- 33. **client:** person entering into a business relationship with the service provider, or who places an order with the service provider to carry out a transaction
- 34. **customer due diligence:** identification, risk rating of the client, verification of identity, experiencing and continuous monitoring of the business relationship and the purpose and nature of the transaction order,
- 35. **transaction:**
 - a) an operation comprising a part of a service provided under business relationship by the service provider within its professional activities, or
 - b) transaction order
- 36. **transaction order:** such case that is a temporary relationship established by contract between a client and a service provider pertaining to the services of the service provider falling within its professional activities,
- 37. **business relationship:** a long-term relationship established by contract for the service within the activities of the Service Provider.
- 38. **verification of source of funds:** client declaration presenting the source of the client financial assets, including the material and immaterial assets
- 39. **virtual currency:** digital display of values not issued or guaranteed by a central bank or public administration; does not have the legal status of a legal tender; it can be stored electronically, accepted as an exchange value, so it is especially electronically transferable and suitable for electronic trading.

V. CUSTOMER DUE DILIGENCE DUTY AND IMPLEMENTATION OF MEASURES

V.1. The customer due diligence duty

The Service Provider shall carry out a due diligence with regard to its clients:

- a) by the establishment of long-term business partnership,

- b) by completion of a transaction order at or above HUF 4,500,000,
- c) in the event of data, fact or circumstance giving rise to a suspicion of money laundering or terrorist financing, where the client has not yet been subject to a due diligence,
- d) when there are doubts about the veracity or adequacy of previously obtained client identification data,
- e) where a change to the client identification data is being implemented and the repeated performance of the customer due diligence becomes necessary based upon the risk sensitivity approach.

The value of the transaction orders shall be added up for those transactions where it can be established that the same client places an order for the same subject matter within the same year. The due diligence obligation thus also extends to several transaction orders that are actually related to each other in the case of ad hoc transaction orders, if their combined value reaches the legal limits. In this case, the due diligence shall be performed upon acceptance of the transaction order by which the total value reaches the threshold.

The Service Provider sets that, in the course of the transaction orders, it shall be subject to a customer due diligence duty only by the performance of transaction orders that reach or exceed HUF 4,500,000. The Service Provider however decides, for the purpose of a possible broadest prevention and combating of money laundering and terrorist financing, to apply interim measures for the transactions at or above HUF 300,000 that makes it possible to have a more precise identification of the client and the orders, and to monitor the clients with regular transaction orders.

V.2. Interim measures

The Service Provider shall be entitled to apply the following interim measures according to its case-by-case assessment in case of transactions at or above HUF 300,000:

- checking of the client's identity based on the client's personal data, documents suitable for verifying personal data provided as specified in paragraph V.3.3, as well as providing e-mail address and telephone number, in person or electronically, via the Service Provider's website,
- completion of client identification data sheet, the politically exposed person declaration and, in the case of non-natural person (organizational) clients, the beneficial owner Declaration among the forms specified in the annexes to this Policy.

V.3. Customer due diligence measures

As part of the customer due diligence, the Service Provider implements the following measures:

- i. identification of the client, recording of personal data,
- ii. the risk rating of the client (in writing in case of possible establishment of a long-term business relationship),
- iii. verification of identity, validity and authenticity check with regard to the documents that have been presented by the client, the assignee thereof, the authorized representatives, and proceeding representative thereof,
- iv. learning and continuous monitoring of the business relationship and the purpose and characteristic of the transaction order, conduction of enhanced procedure (in cases specified in the Policy)
- v. identification of the beneficial owners of the organizational client, declaration regarding the status of the beneficial owners as politically exposed persons,
- vi. Query from the beneficial ownership register
- vii. Difference signal
- viii. recording of data on the source of the funds involved in the transaction relationship, examination of the documents submitted to verify the data;
- ix. if necessary, the verification of the source of funds involved in the business relationship and the examination of the documents submitted for verification.

V.3.1. Identification and verification of identity

During the identification, the Service Provider shall record the following data regarding the client, the assignee, the representative and the authorized representative thereof:

I. In case of natural persons

- a) surname and forename,
- b) surname and forename by birth,
- c) nationality,
- d) place, date of birth,
- e) mother's birth name,
- f) home address, habitual residence in the absence thereof,
- g) type and number of identification document

II. In case of legal person or unincorporated organization

- a) official name of the organization,
- b) registered seat, address of the Hungarian branch in case of foreign undertaking,
- c) main activity (taking into account the registered main activity, as well as the main activity that can be considered as the primary income-generating activity in terms of income)
- d) The identification data of a natural person entitled to represent an organization (in the case of joint representation, of all those entitled to the necessary representation), if they have a delivery agent, the identification data thereof,
- e) company registry number in case of legal person registered in the company registry, resolution number of establishment (registration) or registration number in case of other legal persons
- f) tax number
- g) identification data as regards the beneficial owner of the organization (in accordance with the first subparagraph of this paragraph).

In case the contractual legal relationship shall be considered as long-term business relationship, the Service Provider furthermore shall record:

- a) the type, scope and duration of contract,
- b) for the purpose of specifying the manner of the due diligence, the fact that the risk rating of the client is normal, high or low,
- c) circumstances of the performance (place, date, manner),
- d) information regarding the purpose and nature of the business relationship
- e) information regarding the source of funds based on risk sensitive approach, and the underlying documents.

The Service Provider shall obtain those data from the client that are necessary for the establishment of the identity, by means of the identification form as set out in Annex 2 and shall record it on the form or in the Service Provider's electronic client data base.

In the case of foreign natural and legal persons, efforts should be made to record the broadest possible range of data listed above, provided that, the certificate that embodies an authorization to reside in Hungary or the document evidencing the right of residence shall be also requested (if any) in case of foreign natural persons, while in the case of foreign legal persons it is appropriate to use the site https://e-justice.europa.eu/489/EN/business_registers_search_for_a_company_in_the_eu?init=true for queries.

The above data may also be recorded by means of an audited electronic means of communication.

The Service Provider shall undertake to perform its obligations regarding the verification of the identity within 48 hours upon the receipt of the data provided by the client and to provide the client with information regarding the results of the verification.

V.3.2. Identification of the order

Upon the conclusion of the order, the Service Provider may record the type, period, scope of order in connection with the completion of the transaction

1. value of the transaction, including the value of the virtual and legal tender,
2. the conditions of completion (place, date, method), if it is necessary for the identification of the client and the order (on the basis of the nature and value of the order and the client's circumstances for the prevention and combating of money laundering and terrorist financing).
3. If the Service Provider deems it necessary under the AML Act, the indication of the source of funds for the purchase of virtual tenders in case of transaction orders as well.

Based on the risk sensitivity approach, the Service Provider shall be entitled to request information regarding the transaction related source of funds in the case of transaction orders and the origin of the assets, as well as the presentation of documents thereto.

V.3.3. Documents to be submitted

For the purpose of verification of identity, the Service Provider shall be obliged to require the production of the following documents, as well as to check validity thereof:

In case of natural person:

1. official document (containing a photograph of the person) or passport suitable for identification purposes and official address card for Hungarian citizens, the latter is necessary if he / she has a permanent address or reside in Hungary,
2. passport or personal identification document for foreign nationals, if it embodies an authorization to reside in Hungary, document evidencing the right of residence or a valid residence permit; official address card for Hungarian address, if he / she has a permanent address or reside in Hungary, or the official verification of a Hungarian accommodation.

In the case of a legal person, an organization without legal personality, in addition to the production of the above-mentioned document of the person authorized to act in its name or on its behalf, the document, not older than thirty days, certifying that:

1. the company has been registered by the court of registry, or that the application for registration has been submitted; in case of self-employed persons, the self-employed activity has been notified or the certificate of registration has been issued,
2. the registration has taken place, if its establishment requires a registration by an official body, a bar of association or a court,
3. the entry or registration of the foreign legal person or organization without legal personality has taken place under the national law of its own country.

In case of an application for a company, a registration by an official body, a bar of association or a court:

1. the deed of foundation of the legal person or organization without legal personality prior to its submission to the court of registry, authority, bar of association or court. (In this case, the legal person or organization without legal personality shall provide documental verification about the company, official or judicial registration within 30 days thereupon, and the Service Provider shall record the company registration number or other registration number.)

Identity documents of a natural person is invalid, if

- i. it is not capable of establishing a person's identity, it has been damaged or falsified,
- ii. data in the identity document has been changed,
- iii. the bodies authorized for issuance has withdrawn that,
- iv. its validity is expired,
- v. the entitled died,
- vi. the address data entered in the identity document is invalid, thus it is marked as invalid, or fictional in the address register.

The verification of the maiden surname and first name, citizenship and mother's maiden name data can be omitted if the document presented for verification of identity does not contain it. In this case, it is necessary to record that if the identification data was recorded without verification.

For the verification of the identity, the Service Provider (may) make a paper based or electronical copy of the document produced by the client in order to prevent and combat the money laundering and terrorism financing, to duly perform the duties under the AML Act, to fully complete the customer due diligence, and to ensure effective supervisory activity.

The presented document shall be considered invalid in case of a company subject to the Civil Code, in particular, if it can be established based on the document that:

- i. there is no countersign on the document by the attorney or the legal counsel of the founder, or
- ii. it has not been attested by notary,

- iii. the deed of foundation does not contain the company name, main activity, subscribed capital of the company, or
- iv. the financial consideration of the members (shareholders),
- v. the company's activity is against the legislation,
- vi. all the members (shareholders) participating in the establishment of the company, were legally incapacitated, or
- vii. the participants to the establishment of the company have breached the rule on the minimum number of members,
- viii. in the case of a limited liability company and a public limited company, the legal requirements regarding the minimum amount of the subscribed capital have been breached.

These provisions shall apply to other organizations if it is obvious based on the deed of foundation that it is not suitable to be registered.

V.3.4. Procedure of representatives

If the client wishes to submit the order via an agent, the proxy must be subject to special care. During the verification of the identity, the validity of the assignment, the authorized person's right for disposal, as well as the agent's authorization for representation must be checked.

The assignee must provide the Service Provider with a private deed with full probative force to identify his / her rights to act, and both the data necessary for the identification of the assignor and his / her identity.

The representative or guardian must also be subject of identification in case of a person with limited or no capacity.

V.3.5. Identification of beneficial owners

During the customer due diligence, the representative of the natural person and the legal person or unincorporated organization client shall be required to make a written declaration or to submit a declaration via an audited electronic means of communication as per Annex 2, whether he / she proceeds on behalf or for the benefit of the beneficial owner. The client representative of a legal person or an organization without legal personality shall be obliged to list in its statement all natural persons specified in the definition of beneficial owner of this policy as beneficial owner.

The below data of the beneficial owner must be recorded in the declaration:

- 1. surname and forename,
- 2. surname and forename by birth,
- 3. nationality,
- 4. place, date of birth,
- 5. home address, the residual address in the absence thereof,
- 6. nature and level of ownership interest, if the client is a legal person or an unincorporated organization.

The data on the identity of the beneficial owner must be verified on the basis of the presented document, publicly accessible register, the register of beneficial owners or other register, whereby the Service Provider is entitled to request data from the operator thereof by law. If the information cannot be authenticated based on a publicly accessible register, the Service Provider shall be obliged to verify the authenticity of the information in accordance with the client's additional data provision, as far as necessary. If the authenticity of the information cannot be established due to the lack of necessary documentation, the Service Provider shall refuse to provide the service.

Representative of the Service Provider carrying out customer due diligence shall especially have doubts as to the identity of the beneficial owner or the person exercising effective control in the following cases:

- i. The company has such a foreign registered organization member, the natural person owners of which, included in the declaration, cannot be verified for the service provider on the basis of the presented document, a public database or another authentic database accessible to the service provider,
- ii. The executive officer is also a member of the client company, but is not empowered to make a declaration alone at the time of concluding the contract, but another person accompanying him /

her declares on behalf of the company at the service provider, whose link to the company is not certified by means of company documents or he / she receives the necessary information for the answers via telephone,

- iii. The executive officer is also a member of the client company, but based on his / her appearance and abilities, it shall not be assumed that he / she would fit for the performance and supervision of the tasks falling within the scope of the company's activities,
- iv. Such person acts as client representative before the Service Provider, who, based on the available information, assignments, can be assumed to exercise the factual control, since the executive officer of the company is not available for the Service Provider,
- v. The client organization is included in the list of data providers with an uncertain or unreliable rating.

If the beneficial owner of the client of the legal person or organization without legal personality is the senior official, the senior official must be identified and the verification of his identity must be carried out.

The Service Provider shall record and register the measures taken for the identification and verification of the identity of the beneficial owner.

V.3.5.1 – Specification of the beneficial owner and recognition of complex ownership structures

In cases where the client's owners include non-natural persons, natural persons who have and maintain a 25 % share or voting right throughout the ownership chain, have a real influence on the client's decisions and activities, shall be considered by the specification of the beneficial owner.

If there is any doubt as to the identity of the beneficial owner, the client shall be called to make a repeated declaration about the beneficial owner.

V.3.5.2. Query from the register of beneficial owners and difference signal

The Service Provider shall be entitled (or, in the cases specified below, obliged) to query the register of beneficial owners.

A query from the register of beneficial owners is necessary in the following cases:

- in case of a complex, complicated ownership structure,
- if doubts arise regarding the identity of the beneficial owner of the Service Provider's client,
- if the Service Provider records the beneficial owner(s) data without making the client's representative declare thereabout.

V.3.6. Politically exposed person status

The Service Provider shall acquire the client's declaration by means of forms set out in Annex 5, whether he / she or the beneficial owner shall qualify as a politically exposed person, a close relative thereof or a person in close relation therewith. The declaration shall include the point whereunder he / she shall qualify as a politically exposed person, a close relative thereof or a person in a close relation therewith. The statement must also include information regarding the source of funds.

If, based on the beneficial owner's statement, the beneficial owner shall be classified as a politically exposed person, a close relative thereof, or a person in a close relationship therewith, the following screening measures must be implemented:

1. the client must be classified as high risk,
2. a statement regarding the source of funds and source of assets and an underlying document thereon must be obtained from the client,
3. the business relationship is subject to a management decision as per paragraph V.3.8,
4. the client relationship (if it is considered a permanent business relationship) must be monitored in an enhanced procedure.

V.3.7. Other rules

If the Service Provider, for any reason, is unable to complete customer due diligence measures, it shall refuse to establish any business relationship and to complete a transaction order on behalf of the client concerned or shall terminate the business relationship therewith. This shall include especially but not exclusively the case if:

1. the client does not consent to the establishment of its identity, or does not provide data for this purpose
2. the client cannot present valid documentation for the completion of the identification, or
- e) the Service Provider may determine within the course of the due diligence that the loss, theft or destruction of the ID card has been reported, and the fact that it was found or returned is not registered
- f) data, facts or circumstances indicating money laundering or terrorist financing may arise, or some other critical circumstance is detected.

There is no need for repeated customer due diligence measures, if

- i. upon other business relationship or transaction order, the Service Provider has already performed the customer due diligence concerning the client, the agent, the proxy, the representative and the beneficial owner,
- ii. the Service Provider has previously established the identity of the customer, the agent, the proxy, and the representative in connection with this business relationship or transaction order, and
- iii. there has been no change in the data available, or
- iv. less than 365 calendar days passed since the closure of the previously completed identification.

Simultaneously with the implementation of the customer due diligence measures, the Service Provider shall draw the clients' attention to the fact that during the business relationship the client shall provide the Service Provider with a notification of any changes in the data provided in the course of the customer due diligence or regarding the beneficial owner, within 5 working days becoming aware thereof.

V.3.10. Cases of termination of business relationship

Establishment of business relations shall be forbidden, furthermore the concerned business relationship shall be terminated, and the transaction cannot be completed, if result of the customer due diligence ordered by the AML Act is not fully available for the Service Provider, thus, when the customer due diligence can not be fully performed, i.e:

- the client refuses to provide the personal identification data and documents,
- the client refuses to make the declaration on the status of politically exposed person and the beneficial owner, or the content of the declaration cannot be verified in a satisfactory manner,
- there are still doubts with regard to the personal identification data, the beneficial owner even after the repeated declaration of the client (made in written form or via audited electronic means of communication),
- there is no satisfactory clarification with regard to the sources of funds.

V.4. Simplified customer due diligence (SDD)

The Service Provider shall be entitled to perform a simplified customer due diligence in case of **low risk factors**.

The below data shall be mandatory to be recorded in case of simplified due diligence:

In case of natural person:

1. surname and forename,
2. surname and forename by birth,
3. nationality,
4. place and date of birth,
5. mother's birth name
6. permanent address, residual address in the absence thereof
7. number and type of identifying document

In case of legal person or unincorporated organization:

1. name, shortened name,
2. registered office, the address of the Hungarian branch in case if undertaking with foreign registered office, if it has such,
3. main activity,
4. name and position of representatives,

5. data capable to identify the delivery agents,
6. company registry number, or the resolution number of establishment (registration) or registration number in case of other legal persons,
7. tax number
8. data concerning natural person(s) beneficial owner(s) in accordance with the above list.

The client may also send a copy of the identification documents and declarations under this Policy to the Service Provider by post or by means of electronic communication, as personal hand over is also available.

V.5. Enhanced customer due diligence (EDD)

Service Provider shall be entitled to carry out an enhanced customer due diligence in case of higher risk factors.

The following measures must be implemented within the frame of an enhanced procedure:

- a management approval is needed for the transaction order and the establishment of the business relationship,
- business relationships (including client relationships with regular transaction orders) must be continuously monitored in an enhanced procedure,
- on the basis of a risk sensitivity approach, information on the source of the assets and funds of the client's can be requested and must be requested in relation to the beneficial owner(s) from high-risk third country with strategic deficiencies, or a politically exposed person, or a close relative thereof or a person in a close relationship therewith,
- verification of the identification as regards a beneficial owner can also be carried out within the frame of a personal appearance,
- in case of remote identification- in the absence of personal appearance -, customer due diligence shall be on the basis of authentic/certified copies.

V.5.1. Client personally not appearing

Except for the case of a simplified customer due diligence, and provided that the due diligence is not completed by a secured, protected, pre-audited electronic means of communication operated by the Service Provider, a certified copy of the documents containing identification data must be requested in all cases, if the client, the proxy, the representative or the assignee has not appeared in person for the purpose of identification and verification of identity.

A certified copy of the document may be accepted for identification and verification of identity, if:

- it has been certified by a notary public or by a Hungarian foreign mission in accordance with the relevant provisions of Act on Notaries Public on the attestation of certification of copies, or
- the copy was prepared by an authority of the country where it was issued, if such authority is empowered to make certified copies and - unless otherwise provided for by an international agreement - the competent Hungarian foreign mission has provided a confirmatory certification of the signature and seal of the said authority.

V.6. Customer due diligence carried out by other service provider

The Service Provider shall be entitled to accept the results of a customer due diligence performed by another service provider if the customer due diligence was performed by a service provider with a registered office, branch or premises in the territory of Hungary or in another Member State of the European Union. If the customer due diligence was performed by a service provider having a registered office, a branch or premises in a third country, such result is acceptable in case the service provider applies the customer due diligence and registration requirements established in the AML Act or equivalent, and the supervision of such service provider is also subject to requirements specified in the AML Act or equivalent, or its registered office, branch or premise is in such a third country that has requirements equivalent to the AML Act.

The Service Provider shall not be entitled to accept the result of the customer due diligence if the customer due diligence was performed by a service provider having its registered office, branch, or premises in a third country which shall qualify as a high-risk third country with strategic deficiencies.

VI. IMPLEMENTATION OF FINANCIAL AND ASSET RELATED RESTRICTIVE MEASURES (SANCTION AND EMBARGO)

The Service Provider shall continuously monitor the issuance and subsequent amendments of Union legal acts and UN SC resolutions ordering financial and asset related restrictive measures and other sanction or restrictive measures. The Service Provider shall implement a screening process within a screening, monitoring system to ensure the asset related restrictive, sanction measures.

The Service Provider must refuse to provide any service to a person who or that is subject to a restrictive or sanction measure.

VII. DATA PROTECTION, REGISTRATION

The Service Provider may access and process the personal data obtained during the performance of its obligations related to the prevention of money laundering and terrorist financing - including information on the source of funds and assets - solely for the purpose of performing its tasks arising from the AML Act, to the extent necessary for their performance. From the termination of the business relationship or the completion of the business order, the Service Provider shall be entitled and obliged to register and manage the data, declarations and copies of documents recorded during the customer due diligence for 8 years (until the authority is contacted, but a maximum of 10 years). The Service Provider shall record the rules of its activities involving the management of personal data in a separate data management information sheet, which can be found on the Service Provider's website.

THIS POLICY IS PREPARED WITH REGARD TO THE LEGAL PROVISIONS CURRENTLY IN EFFECT AND TO THE SERVICE PROVIDER'S CURRENT RISKS, THE SERVICE PROVIDER MAY – ESPECIALLY UPON CHANGES THEREOF – UNILATERALLY AND UNLIMITED AMEND AND WITHDRAW THE POLICY.

Budapest, November 01, 2022

Tiwala Solutions Kft.