Interactive Brokers Central Europe Zrt.

INFORMATION

on Client Identification Procedures

Valid from: 07 December 2022

1. Client identification and rating

Prior to the provision of services, Interactive Brokers Central Europe Zrt. (hereinafter referred to as: 'IBCE' or 'the Company') shall perform Client due diligence in full compliance with the laws in effect from time to time.

Client due diligence shall be performed by the Company in compliance with the laws in effect on the prevention of money laundering, in particular the provisions of Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (hereinafter the Anti-Money Laundering Act).

In the cases outlined below, the Company shall perform the following with respect to Clients (including their proxy, the party authorised to dispose over the account and the person acting as representative on behalf of the Client): identification, risk-based rating, the verification of identity, obtaining information on the purpose and nature of and monitor the transaction order (client due diligence).

2. Mandatory client due diligence

In the cases specified below the Company shall perform client due diligence measures with respect to Clients (including their proxy, the party authorised to dispose over the account and the person acting as representative on behalf of the Client):

a) At the time of establishing the business relationship.

b) If data, facts or circumstances implying or suggesting money laundering or the financing of terrorism arise, provided that the client due diligence set out in paragraph a) has not yet taken place.

c) In addition to the cases outlined above, the Company shall also complete client due diligence in the event of any doubt as to the authenticity or appropriateness of client identification data. This shall include the case where the data of the client (e.g. name, domicile, registered office, etc.) or the ownership structure of a non-natural person client changes. In the event of a change in the management or representatives of a non-natural person client, it shall be verified whether or not the data recorded during the client due diligence or the circumstances serving as a basis of the beneficial owner declaration remained the same.

d) If a change was recorded in client identification data and if the risk sensitivity approach requires the client due diligence to be repeated.

In the event of cases set out in Section 15 of the Anti-Money Laundering Act, the Company shall record the data specified in Section 7(2) and, in order to verify personal identity, it may also request that the documents stipulated in Section 7(3) are presented.

There is no need to repeat the client due diligence if:

a) the Company has already completed such client due diligence in connection with another business relationship or transaction order in relation to the Client, their proxy, the party authorised to dispose over the account and the person acting as representative on behalf of the Client, and

b) in the context of this business relationship or transaction order, the personal identity of the Client, their proxy, the party authorised to dispose over the account and the person acting

as representative on behalf of the Client was already verified, and

c) no changes have been made to the data required to be provided under the Business Rules and the Money Laundering Policy.

3. Possible methods of client due diligence at the Company

The Company may conduct client due diligence in any of the following manners:

a) By sending the necessary documents and making the required statements, without appearing in person, through the electronic client identification portal of the Company.

b) By sending the necessary documents, without appearing in person. In this case, the Client must send their documents and declarations to the Company in a certified copy format. Certified copies of documents may be obtained from notaries public, the Hungarian foreign delegation authority or the authority authorised to issue certified copies at the place of issue of the document. In case of foreign documents, provided that no bilateral treaty on the acceptance of documents is in place between Hungary and the state where the document was issued, the Hungarian foreign delegation authority shall testify, by issuing an apostille, that the authority that issued the certified copy of the document is authorised to do so. For signatory countries of the Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents (signed on 5 October 1961), legalisation may take place by obtaining a so called apostille. The Company shall only accept documents drafted in Hungarian and English and requires a certified translation for documents in any other language to be accepted.

c) Via a certified payment account. According to the sub-case of case b), client due diligence may also be conducted with Client documents and declaration via fax or electronically without certification, if the Client's payment account (bank account) is also certified simultaneously. In such a case the Company shall contact the institution managing the payment account and request confirmation with respect to the data of the Client. In such a case the Client will be able to use their client account opened with the Company only in a limited manner. As long they are not identified using another client-identification method, they may only transfer or withdraw funds to and from their bank account covered by this clause. If the payment account managing institution specified by the Client is a foreign service provider and does not confirm the Client data within the due date, the Company shall grant a 15-day period for the Client to have them vetted with another method. Should the due date be frustrated, the Company shall suspend the business relationship and, furthermore, refuse to disburse any funds to the payment account specified by the Client until client due diligence has taken place or the account manager service provider has confirmed the Client data.

d) Accepting the results of client due diligence from another service provider. The Company may accept the results of client due diligence from certain partner institutions.

e) The Company is entitled to perform the Client's due diligence process with secure and protected, pre-audited electronic communications device operated by the Company, based on the Anti-Money Laundering Act and Decree No. 26/2020 (VIII.25.) of the Central Bank of Hungary. The Company applies the due diligence via direct (video due diligence) and indirect ways of electronic means of communication.

   The Company applies video due diligence (direct way of electronic means of communication) on a risk-based approach or if the Client's total equity reaches or exceeds

the 10 million HUF threshold (~24.000 USD), the Client is invited to perform the video due diligence within a specified 2-week period. If the Client fails to have a successful and approved video due diligence call within the specified 2-week period, the Company may place restrictions on the Account, including but not limited to restricting the opening of new positions. The restriction does not affect closing remaining open positions. The exact rules of this process are detailed in the 11. Point of this document.

The Company applies due diligence via indirect way of electronic means of communication on a risk-based approach if the due diligence as point a) cannot be applied. In the course of the indirect due diligence, after the consent, the Client is asked to take pictures of the document and to take a selfie via a web-based website. The exact rules of this process are detailed in the 12. Point of this document.

4. Unsuccessful client due diligence

In the event that the Company is unable to perform the client due diligence required by law and the Company's internal policies, it shall refuse to establish a business relationship and to execute transaction orders or terminate the business relationship with the client.

5. Identifying and verifying the identity of natural persons, postal (mailing) address

For the purposes of verifying the identity of a natural person, the Company shall request that the following documents are presented:

a) the official document (ID card, passport and card format driving licence) of the Hungarian citizen suitable for the verification of identity and the official address card,

b) in the case of foreign citizen natural persons, their travel document or ID card, provided that,

c) such documents authorise the relevant person to stay in Hungary, the document certifying the right of residence or the document authorising residence, the official card certifying Hungarian domicile provided that the domicile or the residence is in Hungary.

As part of the identification, the Company shall record the following data of the natural person:

a) surname and forename,
b) surname and forename at birth,
c) citizenship,
d) place and date of birth,
e) mother's name at birth,
f) domicile or, if there is none, residence,
g) the type and number of their identification document.

The Company shall record and register data in paragraphs a) to g) pursuant to its statutory obligation. If the Client is a politically exposed person or a close relative or a closely related person thereof, in addition to the above data, the source of the funds shall also be recorded under the law.

6. Identifying legal persons or entities without legal personality and verifying their identity

In case of legal persons or entities without legal personality, the Company shall, in addition to the document of the person authorised to act for and on behalf of such entity and also the

specimen signature (or the foreign equivalent of the same) certifying in a credible manner the power of such person to sign for such entity referred to Section 5 above, request a document (of less than 30 days old), that

a) the company incorporated in Hungary was registered by the Court of Registration, or that the company has submitted their application to this effect; in the case of a sole proprietor the fact that their sole proprietor's licence was issued or that the certificate of registration was issued,
b) in case of legal entities that are established under Hungarian law, but are not covered by paragraph a), the legal entity has been registered, provided that such registration by either an authority or a court is necessary for such establishment,
c) in case of foreign legal entities or other entities without legal personality, such entity has been registered under the laws of their own country
d) in case of legal entities or other entities without legal personality that have not yet submitted their application for registration, the establishment of such entity is proven with the instrument of incorporation.

Prior to the submission of their application seeking registration to the Court of Registration, authority or court, the Company shall request the legal entity or the entity without legal personality to submit their articles of association (articles of foundation, statutes). In such a case, the legal entity or other entity without legal personality shall submit a document within 30 days following registration by the Court of Registration, authority or court proving that company registration or registration took place; then the Company shall record the company registration number or other registration number.

During the course of due diligence, the Company shall record the following data of a legal entity or another entity without legal personality:

a) name, short name,
b) the address of their registered office and/or (in the case of a business with a foreign registered office) the address of the Hungarian branch,
c) core activity,
d) the name and position of the people who hold a representation right,
e) the full name and address (or, there is none, the place residence) of the agent for service of process, if there is any,
f) in case of legal entities included in the company register: their company registration number or in the case of other legal entities: the number of the resolution or registration about their establishment (registration, recording,
g) tax number.

7. Beneficial owner declaration

For client due diligence, the natural person Client shall deliver a written declaration, provided they act for and on behalf of the beneficial owner. Regarding the beneficial owner, the Company shall request that the following data are provided:

a) surname and forename,
b) surname and forename at birth,
c) domicile or, there is none, the place of residence,
d) citizenship,
e) place and date of birth.

In case of doubt as to the identity of the beneficial owner, the Company shall take all further measures specified by the Central Bank of Hungary until it can satisfy itself as to the person of the beneficial owner.

The Company shall verify the data concerning the personal identity of the beneficial owner based on the document presented, a publicly accessible register or based on a register from the controller of which the Company may request data under the law.

For client due diligence, the legal representative of the legal person or entity without legal personality shall, based an accurate and timely records kept by the client, make a written declaration about all beneficial owners of the legal entity or entity without legal personality. Regarding the beneficial owner, the Company shall request that the following data are provided:

a) surname and forename,
b) surname and forename at birth,
c) citizenship,
d) place and date of birth,
e) domicile or, there is none, the place of residence,
f) the nature and extent of ownership interest.

Beyond the generally applicable rules of the Anti-Money Laundering Act on identifying beneficial owners as persons having at least 25 percent ownership interest in legal persons or entities without legal personality, , the Company is entitled, on a risk-based approach, to identify owners of legal persons or entities without legal personality with at least 10 percent ownership interest as beneficial owners.

If the beneficial owner is a managing officer within the meaning of Section 3(38)f) of the Anti-Money Laundering Act, the Company shall also identify the managing officer and conduct verification on its identity. The service provider shall record the client due diligence, including also the information if such due diligence could not be performed.

In case of doubt as to the identity of the beneficial owner, the Company shall take all further measures specified by the Central Bank of Hungary until it can satisfy itself as to the person of the beneficial owner. Such measures include that the Company may request the Client to give all the information specified in 2.5.1 and 2.5.2 for all of its owners irrespective of the proportion of their ownership or voting rights or any other interests.

The Company may verify the data concerning the personal identity of the beneficial owner based on the identification document presented, a publicly accessible register or based on a register from the controller of which the Company may request data under the law.

8. Determining on Politically Exposed Person status for Clients and Beneficial Owners

For natural person clients and beneficial owners of legal person clients or entity clients without legal personality the Company determines whether or not, under the law of their own country, they should be considered as a politically exposed person, a close relative of a politically exposed person or a person closely related to a politically exposed person under Section 4 (2) of the Anti-Money Laundering Act.

If the natural person client or the beneficial owner qualifies as a politically exposed person, he/she needs to declare the information concerning the source of the funds and source of wealth in a separate declaration.

In the case of a politically exposed person, the business relationship can only be established after an approval was granted by a senior manager specified in the Company’s internal policy for substitution.

Politically Exposed Person: any natural person who holds an important public function or held an important public function in at least the year preceding the performance of the customer due diligence measures.

Persons holding an important public function:

a) the head of state, the head of government, ministers, vice-ministers, secretaries of state, in Hungary: the Head of State, the Prime Minister, ministers, secretaries of state,
b) Parliament representatives and members of similar legislative bodies, in Hungary: Parliament representatives and nationality spokesmen,
c) members of the governing body of political parties, in Hungary: members and officers of the governing body of political parties,
d) members of the supreme court, the constitutional court or any high-level judicial body whose decisions cannot be appealed against, in Hungary: members of the Constitutional Court ("Alkotmánybíróság"), Courts of Appeal ("ítélőtáblák") and the Supreme Court ("Kúria"),
e) members of the Board of Directors of the court of auditors and the central bank, in Hungary: the Chair and Vice Chair of the State Audit Office ("Számvevőszék"), the Monetary Council and the Financial Stability Council,
f) ambassadors, chargés d'affaires and high-ranking officers of armed forces, in Hungary: the head of the central body of the policing body and his/her deputy, as well as the Chief of Staff of the Hungarian Defence Forces and his/her deputies,
g) members of the directing, controlling or supervisory bodies of undertakings in the majority ownership of the state, in Hungary: the executive officers of undertakings in the majority ownership of the state and the members of the managing bodies of such undertakings having management or supervisory powers,
h) heads of international organisations, their deputies and members of the managing bodies of such organisations or any person holding an equivalent function.

Close relatives of a Politically Exposed Person: the politically exposed person's spouse or partner; biological, adopted, step- or fostered child and any spouse, partner of biological, adopted, step- or fostered child as well as the politically exposed person's biological, adopter, step- or foster parents.

A person in close relations with a Politically Exposed Person:

a) any natural person who is the beneficial owner of a legal person or organisation without legal personality jointly with any of the persons holding an important public function, or is in a close business relationship with such a person;
b) any natural person who is the sole owner of a legal person or organisation without legal personality established for the benefit of any of the persons holding an important public function.

Based on the above declaration, the Company shall take the measures necessary to verify the data either in the register available for this purpose or in a publicly accessible register.

In the case of a politically exposed person, the business relationship can be established, and the transaction order can only be executed after an approval was granted by either the Chief Executive Officer of the Company or the persons specified in the Company's internal policy for substitution.

9. Obligation to give notice on changes of identification data

During the business relationship, the Client is required to notify the Company concerning any change in the data and information supplied in course of identification or those concerning the beneficial owner within five working days of the day when such information is received.

10. Making copies of the presented documents

For the purpose of verification of identity the Company is obliged by law to make copies of the presented official documents containing data set out in Sections 5 and 6 of the Anti-Money Laundering Act, including all personal data recorded in the official document. By copy, scanned documents, photos, and photos made with a camera also meant.

11. Customer due diligence via video call (direct way of electronic means of communication)

The Company is entitled to perform the client's due diligence process with secure and protected, pre-audited electronic communications device operated by the Company, based on the AML Act and Decree No. 26/2020 (VIII.25.) of the Central Bank of Hungary (hereinafter: Decree).

The Company records all communication between the Company and the Client during the customer due diligence, the detailed information on the Client's customer due diligence via video call and the Client's expressed consent to that in images and recordings in a retrievable way and makes it available to the Client upon request.

During the video call, the following documents will be requested by the Company to be presented:

a) for Hungarian nationals:
   - passport, personal identity card or driver's license
   - and – if having a Hungarian residential address – the official address card issued by the Hungarian authorities

   (hereinafter: ID card)

b) for non-Hungarian nationals:
   - passport or personal identity card
   - and – if having a Hungarian residential address – the official address card issued by the Hungarian authorities

   (hereinafter: ID card)

During the customer due diligence, the Client is requested to
a) look at the camera so that his face can be recognized and recorded,
b) to convey in an understandable manner the document identifier of the ID card used for the customer due diligence, and
c) move the ID card in such a way as to identify and record the security elements and datasets that are on it.

During the video call, the Company will verify that the ID card is suitable for the customer due diligence procedure, thus
a) certain elements of the ID card and their location correspond to the requirements of the issuing authority,
b) each security element, in particular the hologram, the kinegram, or other security features identical to it, are recognisable and free of damage,
c) the ID card has a field suitable for machine data reading,
d) the ID card's identification number matches the identification number provided by the Client, is recognisable and undamaged.

The Company makes sure during the customer due diligence process that
a) the Client's face is recognisable and identifiable according to the photo on the presented ID card, and

b) the data on the ID card can be logically matched to the customer's data available to the service provider.

During the video call, the two-factor identification is also performed, a randomly generated identification code is sent to the client via SMS, and the client is obliged to enter the identification code, that will be verified by the system.

The due diligence via video call is not successful if

a) the Client withdraws his authorisation for the recoding of data during the customer due diligence via video call,
b) the physical and data content requirements of the documents or documentation presented by the Client are not provided,
c) the visual identification conditions of the Client, the documents or documentation presented by the Client are not in place,
d) the voice and video recording could not be performed,
e) the Customer does not return, or only partially or incorrectly returns, the identification code,
f) the Client does not make a declaration or makes it visibly under influence, or
g) any contradiction or uncertainty arises in relation to it during the proceedings.

The Client will receive the notification of the result of the due diligence process within two working days.

12. Customer due diligence via indirect way of electronic means of communication

The Company is entitled to perform the client's electronic due diligence process with secure and protected, pre-audited electronic communications equipment operated by the Company, based on the AML Act and Decree No. 26/2020 (VIII.25.) of the Central Bank of Hungary (hereinafter: Decree).

The Company records all communication between the Company and the Client during the customer due diligence, the detailed information on the Client's customer due diligence via indirect way and the Client’s expressed consent to it in a retrievable way and makes it available to the Client upon request.

The Company shall carry out the indirect electronic customer due diligence procedure with the audited electronic communications equipment:

a) that is capable to determine whether the customer who appears at the remote location to be vetted is a real person, and uses the audited electronic means of communication by him or herself in real time, and the live feed is not manipulated, and
b) that is capable of comparing the photo taken of the customer during the customer due diligence procedure with the facial image found in the instrument used in the due diligence procedure, in a way from which it can be established beyond doubt whether the individual portrayed in the official document suitable for identification purposes is the same as the one featured in the photo.

During the customer due diligence, the Client is requested to

a) look at the camera – while capturing the selfie photo – so that his face can be recognized and recorded,
b) capture the ID card or passport (hereinafter: ID card) in such a way as to identify and record the security elements and datasets that are on it.

During the indirect due diligence, the Company will verify that the ID card is suitable for the customer due diligence procedure, thus

a) certain elements of the ID card and their layout correspond to the requirements of the issuing

authority,
b) each security element or other security features identical to it, are recognisable and free of damage,
c) the ID card's identification number matches the identification number provided by the Client, is recognisable and undamaged.

The Company makes sure during the customer due diligence process that
a) the Client's face is recognisable and identifiable according to the photo on the presented ID card, and
b) the data on the ID card can be logically matched to the customer's data available to the service provider.

During the indirect due diligence, the two-factor authentication is also performed.

The Company can also perform the indirect customer due diligence by retrieving the authentic, natural identification data, suitable for the identification of the customer, from ID card containing the electronic storage element (NFC chip reading).

The Company ensures during the customer due diligence that
a) the facial image of the customer is recognisable and can be identified with the facial image on the ID card presented by him/her, and
b) the identification data required by the AML Act have been fully obtained and the data on the ID can be logically matched with the data held by the service provider about the customer

The indirect due diligence is not successful if
a) the Client withdraws his authorisation for the recoding of data during the customer due diligence,
b) the physical and data content requirements of the documents or documentation presented by the Client are not provided,
c) the visual identification conditions of the Client, the documents or documentation presented by the Client are not in place,
d) the photo capturing could not be performed,
e) any contradiction or uncertainty arises in relation to it during the proceedings.

The Client will receive the notification of the result of the due diligence process within two working days.

13. Data processing

Related to the financial services (including the auxiliary financial services) and investment services (including the ancillary services) provided and any other services provided by the Bank (as Data Controller), based on the legal requirements stipulated by the Anti-Money Laundering Act and based on the legitimate interest of the Company, the Company processes personal and non-personal data in course of identification and verification of the identity of the customer and during the business relationship.

Information on the scope of personal data and the purpose of the data processing are available in the Data Processing Information of the Company.

For a period of eight years after the end of the business relationship or after the date of carrying out the transaction order, the Company
a) is authorised to process personal data
b) is obliged to keep non-personal data, including all data and information related to business relationship.
The period of data retention may be extended up to ten years as a maximum upon the request

of a competent authority.

The Company is to delete or destroy the data upon the expiry of authorization or obligation to data processing.