The Policy of Dr Nagy Consulting QFC Branch on the prevention and countering of money laundering and terrorist financing, and on the implementation of financial and proprietary restrictive measures ordered by the UN Security Council

adapting

statutory rules applicable within the QFCRA's AML and CFTR regime, including:

- the Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019 (AML/CFTR);
- Administrative Order No. (1-2004) establishing the Qatar Financial Information Unit (QFIU) and its organisational structure;
- Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing;
- Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing;
- Law No. (27) of 2019 Promulgating the Law on Combating Terrorism
- Implementing Regulations of 2020 (Targeted Financial Sanctions)
- Law No. (11) of 2004 (Penal Code of Qatar)
- Law No. (6) 2020 amending Criminal Procedures Code Law No. (23) 2004

Preliminary notes:

The below provisions of this AML policy are applicable to the entire organisation of Dr Nagy Business Consulting QFC Branch, including without limitation their affiliated entities, persons of significant control, directors, employees, agents and third-parties (henceforth referred to as the "firm"), whether employed, contracted or otherwise engaged in professional activities of any kind, whether in the context of consultancy, advisory, commercial, fiduciary, escrow or trustee relationships, while acting for and on behalf of clients or on their own account, both inside and outside of the territories of the State of Qatar.

Correspondingly, the present AML policy sets out binding rules, practices and standards for the conduct of any beneficial owner, member, partner, director, employee, worker, agent or contractor of the firm in relation to combatting money laundering and terrorist financing.

All the statutory obligations and commitments specified hereunder shall be ultimately interpreted and construed in line with and for the purposes of the QFCRA's AML/CFTR regime.

In the event of conflicting regulations intended to govern this AML policy, the currently applicable AML/CFTR legislation of the QFCRA (or the State of Qatar) shall prevail. Should a conflict between any provision of this AML policy and the currently applicable AML legislation occur, the requirements of the legislation that necessitates stricter or additional requirements to ensure and enforce adequate guarantees and levels of security in terms of AML/CFTR shall be applied.

Peter Nagy E, Dr. Ph.D.

Adopted by Founder's Resolution nr. 1/2020.
Effective from: 1 September 2020

Contents

I. THE PURPOSE OF THIS POLICY

The purpose of this Policy (hereinafter: the "**Policy**") is for the **Dr Nagy Consulting QFC Branch** (hereinafter: the "**Branch**") to consolidate the Branch's obligations related to preventing and countering money laundering and terrorist financing based on the "*Anti-Money Laundering and Countering the Financing of Terrorism Rules 2019 (AML/CFTR), Version No. 2, Effective: 15 August 2020*" (hereinafter: the "**AML/CFTR**"), as well as to ensure that all employees of the Branch are able to comply with the due diligence and reporting obligations set out in the AML/CFTR.

II. PERSONAL AND MATERIAL SCOPE OF THE POLICY

The personal scope of the Policy extends to any present or future departments of the Branch, as well as to any employees working in such departments.
The material scope of the Policy extends to the licenced activities of the Branch aimed at preventing and countering money-laundering and terrorist financing, the risk-based classification, due diligence and monitoring of costumers, the implementation of any tasks related to the reporting and registration of suspicious financial transactions, the suspension of transactions, as well as the implementation of financial and proprietary restrictive measures.

III. RELATED LEGISLATION

Related legislation:

- Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019 (**AML/CFTR**) Version No. 2 Effective: 15 August 2020;
- Qatar State Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing
- The financial and proprietary restrictive measures introduced by the UN Security Council.

IV. INTERPRETATIONS

For the purposes of this Policy:

1. **employee**: for the purposes of this Policy, the managing director or employee of the Branch and any assisting family member of these, as well as a person employed or engaged in a mandate in connection with the licenced activities of the Branch;
2. **parent company**: any company that has a controlling interest and influence over the operations of another company;
3. **audited electronic communication device**: an electronic real-time image and sound transmission system suitable for the client's remote due diligence through electronic data transmission channels, for the interpretation of the client's declaration, the safe storage, retrieval and verification of the stored data;
4. **identification**: the recording of the data specified in AML / CFTR Chapter IV in a retrievable manner. The identification data is recorded by the Branch on electronic or paper-based data carriers in a reliable and retrievable manner;
5. **group**: a set of companies comprising of a parent company, its subsidiaries and branches as well as those companies in which the parent company or its subsidiary has a controlling interest or a shareholding;
6. **controlling interest**: a decisive influence used in the definition of a parent company or a relationship between a person and a company pursuant to which

a) the person with control has the capacity to decide about the distribution of the company's profits, the realignment of profit or loss to another company or the company's strategy, business or marketing policies,
b) coordination of the management of the company with that of another company for the purposes of a mutual objective is permitted, regardless of whether the agreement is set out in the articles of association (charter document) of the company or in another written contract,
c) common management is exercised through the management bodies, supervisory boards of the companies comprised of all or some of the same persons (who provide the necessary decision-making majority), or
d) the person with control is able to exercise substantial influence in the operation of another company without any capital involvement;

7. **resolution of the UNSC**: the resolution adopted by the United Nations' Security Council for the maintenance of international peace and security as provided for in Article 25 of the Chapter of the United Nations, promulgated by Act I of 1956;
8. **shell bank:** a credit institution, financial services institution or credit institution, an institution engaged in equivalent activities, established in a state in which it has no head office, and which is unaffiliated with a regulated financial group;
9. **FIU:** means the Financial Intelligence Unit established under the AML/CFT Law.
10. **head office:** the place where the service provider conducts its principal activity and where ultimate decision-making takes place;
11. **official and certified translation**: a proofread, stamped, concatenated translation with an official clause proving that the translation is consistent with the text provided to the translation agency;
12. **unincorporated organisation**: any legal entity other than (incorporated) legal persons and natural persons;
13. **agent for service of process**: if the contracting chief executive of a legal person or an unincorporated organisation does not have a residence in Hungary, it shall be obliged to name a person with a Hungarian address as its agent for service of process. The agent for service of process may be an organisation with a registered seat in Hungary or a natural person with a permanent residence;
14. **politically exposed person:** a natural person who is entrusted with prominent public functions, or who has been entrusted with prominent public functions within at least one year before the implementation of the client due diligence measures, as well as any family member or close associate of such person;
15. **natural person who has been entrusted with prominent public functions:**
    a) heads of State, heads of government, ministers and deputy ministers, state secretaries,
    b) members of parliament or of similar legislative bodies,
    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 may not be subject to further appeal,
    e) members of courts of auditors or of the boards of central banks,
    f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces,
    g) members of the administrative, managing or supervisory bodies of enterprises with majority state ownership,
    h) directors, deputy directors and members of the board of an international organization;
16. **family members of a politically exposed person:** the spouse or domestic partner of a politically exposed person; the biological and adopted children, stepchildren and foster children of a politically exposed person as well as their spouses or domestic partners; the biological, adoptive, step- and foster parents of a politically exposed person;
17. **close associates of a politically exposed person:**

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 politically exposed person;

18. **risk-sensitivity approach**: procedure fixed in the internal policy relying on the outcome of internal risk assessment, based on the nature of the business relationship or on the type and value of the transaction order and on the client's circumstances, for the purpose of preventing and countering money laundering and terrorist financing;
19. **subsidiary:** any company over which another company effectively exercises a controlling influence, on the understanding that all subsidiaries of the subsidiary companies shall also be considered subsidiaries of the parent company;
20. **correspondent relationship**:
    a) the provision of financial or investment services by a credit institution to another credit institution, including providing a payment account, cash management, international fund transfers, check-clearing and foreign exchange services,
    b) the relationship between and among credit institutions and financial service institutions including, in particular, relationships established for securities transactions and payment transactions;
21. **enhanced procedure**: enhanced monitoring including a set of risk-based measures to manage the risk inherent in client, ~~product,~~ service, transaction, used ~~assets~~interface methods, or geographic exposures;
22. **monitoring**: the continuous monitoring of a business relationship;
23. **money laundering**: the term „money laundering" covers all acts and procedures designed to make it impossible to identify the origin of an illegally obtained – inferring a criminal offence – thing, typically money, and to indicate that it is from a legal source;
24. **money laundering and terrorist financing risk**: the probability and effect of money laundering or terrorist financing;
25. **financial intelligence unit**: an organisational unit specified in a separate act;
26. **financial and proprietary restrictive measures**:
    a) the freeze on monetary instruments and economic resources ordered by the act of the European Union or the resolution of the UNSC,
    b) the prohibition of providing monetary instruments set out in the act of the European Union or the resolution of the UNSC; and
    c) prohibition or restrictions on financial transactions (the transfer of monetary instruments) as well as the related authorisation procedure set out in the act of the European Union or in certain cases specified by the resolution of the UNSC;
27. **subject of the financial and proprietary restrictive measures:** a natural or legal person, or an unincorporated organisation subject to Qatari legislation imposing financial and proprietary restrictive measures or the resolution of the UNSC, or a natural or legal person, or an unincorporated organisation, which is a member of an organisation that is the subject of Qatari legislation imposing financial and proprietary restrictive measures or the resolution of the UNSC;
28. **licenced activities** of the Branch:
    - the business activities of company headquarters;
    - the business activities of the provision, formation and administration of trusts and similar arrangements of all kinds;
    - the business of provision, formation, operation and administration of companies; and
    - the business of providing the Professional services of:
      (i) advisory/consulting in relation to strategic consulting; and
      (ii) third party administration, and addition

- designated Non-Financial Business or Profession (DNFBP) as per the AML/CFTR 1.3.3

29. **proliferation-financing**: financial support for the proliferation of weapons of mass destruction as enshrined in Qatari legislation and the resolution of the UNSC;
30. **high-risk third countries with strategic deficiencies**: countries defined in the 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;
31. **official document suitable for identification purposes**: a personal identification document (identity card), passport, and driver's license card;
32. **verification of identity**: the procedure to verify the identity of the client, agent, proxy, other authorized representative, or the beneficial owner.
    During the verification of identity, the Branch shall be obliged to check the validity of the presented documents; in case of an agent, the validity of the power of attorney; while in case of a proxy or authorised person, the validity of the power of representation and power of disposition.
    a) In case of natural persons:
        a. the official document suitable for the verification of a citizen of Qatar (identity card, driving licence card, and passport) and official address card,
        b. 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 in proof of having a home address in Hungary,
    b) in case of legal persons and unincorporated organizations, a document issued within thirty days to date, to verify:
        a. that the domestic economic organisation has been registered by the QFC-CRO or a registration request has been submitted to that end;
        b. in case of other domestic legal persons whose existence is subject to registration by an authority or court, the document of registration,
        c. in case of foreign legal persons and unincorporated organizations, the document proving that it has been entered or registered under the law of the country in which it is established,
    c) the instrument of constitution of legal persons and unincorporated organizations that have not yet been submitted for registration to appropriate authority keeping the registry (deed of foundation, articles of incorporation). In this case, the legal person or unincorporated organisation shall certify in writing that the registration has taken place, within 30 days after the registration, and the service provider shall be obliged to record the registration number of other reference number;
33. **unusual transaction**: a transaction,
    a) that is not in line with the procedures generally followed in relation to a ~~product or~~ service,
    b) that does not have clear economic or legal basis,
    c) in the case of which the frequency and size of the transactions unreasonably change compared to the client's previous activity;
34. **managing director of Branch**: the natural person who is entitled to represent the Branch, exercise decision-making functions on its behalf, or exercise managerial functions within the Branch;
35. **managing director of Branch according to its bylaws**: a natural person who is nominated by the managing director of the Branch in the bylaws by taking into account the following aspects:
    a) they shall have adequate knowledge of the extent to which the Branch is exposed to money laundering and terrorist financing risks; and
    b) they shall have adequate managerial authority to initiate or make decisions concerning risk exposure;
36. **terrorist financing**: the provision or collection of material means to ensure the conditions of an act of terror, or the provision of material means to a person preparing to commit an act of terror or a person in connection to them;

37. **series of related transactions**: the transactions for which the same client places an order within a period of one year under the same title for the same subject matter;
38. **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 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 that has dominant influence on a legal person or in an unconsolidated organisation, namely it is a member or shareholder thereof and it has the right to appoint and recall the majority of the executive officers or supervisory board members of the legal person, or other members of or shareholder in that legal person are committed under agreement with the holder of a participating interest to vote in concert with the holder of a participating interest, or they exercise their voting rights through the holder of a participating interest, provided that together they control more than half of the votes,
    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 foundation's assets,
        ii. where the individuals that benefit from the foundation have yet to be determined, the natural person in whose main interest 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 foundation's assets,
    e) in the case of fiduciary asset management contracts, the following persons:
        i. the principal(s) and the beneficial owner referred to in paragraph a) or b) thereof,
        ii. the fudiciary(ies) and the beneficial owner referred to in paragraph a) or b) thereof,
        iii. the beneficiaries or class of beneficiaries and the beneficial owner referred to in paragraph a) or b) thereof, and
        iv. any natural person exercising effective control over the trust fund via other means, and
    f) in the absence of the natural person referred to in paragraphs a) and b), the executive officer of the legal person or unincorporated organisation (if there are multiple executive officers, all of them);
39. **client**: any person entering into a business relationship with the Branch or places an order with the Branch;
40. **client due diligence**: the performance of due diligence measures set out in AML/CFTR;
41. **transaction**:
    a) an operation comprising a part of a service provided under business relationship by the Branch within its licenced activities; or
    b) transaction order;
42. **transaction order**: a transaction that is an ad hoc legal relationship established between the client and the Branch under a contract concerning a use of service that falls within the scope of the Branch's licenced activities;
43. **business relationship**: a permanent legal relationship established by a contract between the client and the Branch for the use of the licenced activities;
44. **the Branch's senior management responsibilities**: the Branch's senior management responsibilities are ruled as per Part 2.2.1 and 2.2.2 of the AML/CFTR;
~~44.~~45. **Member State**: shall mean a member state of the European Union.

Formatted: English (United Kingdom)

Formatted: Font: Bold

The above definitions cover the definitions relating to the Branch's current and licenced activities, however, for the purposes of this Policy, the definitions of AML/CFTR not listed in this Policy shall apply mutatis mutandis.

PART 1: PROVISIONS CONCERNING MONEY LAUNDERING

V. THE PERFORMANCE OF DUE DILIGENCE OBLIGATION AND IMPLEMENTATION OF MEASURES

One of the tools in the fight against money laundering and terrorist financing is the due diligence process, which works efficiently and effectively if the Branch, at all times, acts in accordance with the principles of 'Know Your Client' (KYC) and 'Client Due Diligence' (CDD).

V.1. The client due diligence obligation

The Branch shall be obliged to perform client due diligence:

a) when establishing a business relationship;
b) when conducting a transaction order for at least EUR 15,000;
c) when any information, fact, or circumstance indicates money laundering or terrorist financing, if due diligence has not been performed yet;
d) if there is any doubt as to the veracity or adequacy of previously recorded client identification data. This includes when some of the client's data (e.g. name, address, registered seat) or the ownership structure of a non-natural person client changes. Should there be any changes in the management or representatives of the non-natural person client, it shall be verified that there has been no change in the data recorded during the client due diligence or in the circumstances on which the beneficial owner declaration is based.

In case of transaction orders, the due diligence obligation shall cover series of related transactions if their combined value is at least EUR 15,000. In this case, due diligence shall be carried out upon accepting the transaction order with a combined value of at least EUR 15,000.

V.2. Client due diligence measures

V.2.1 General rules

The Branch shall ensure that all available data and documents on clients and business relationships are up to date.

The Branch shall ensure that all matters relating to KYC (as per Chapter 4 of the the AML/CFTR) which are applicable to the Branch's licenced activities and due diligence procedures, are included in this section.

To this end, the Branch shall check the available data on its clients every 5 years. If, during the control procedure any doubt concerning the timeliness of data and declarations arises, the client due diligence measures shall be repeated.

The Branch shall state, in the terms and conditions of the contract of services or on the form/beneficial owner declaration used during the client identification, that during the business relationship the client is obliged to notify them about any changes in the data provided to them during the client due diligence, or, regarding the change in the person of the beneficial owner within 5 business days of becoming aware of such change. Clients shall also

be told of their obligation to notify the Branch about any changes in their data or the data of the beneficial owner within 5 business days.

If there is any change in the client's data and the client does not notify the Branch in writing as required, the change in data shall be recorded upon the client being present in person.

The verification of clients' and the beneficial owner's identity shall be carried out before the business relationship is established or the transaction order is conducted. The verification may also be carried out during the establishment of the business relationship should that be necessary to avoid the disruption of the normal course of business, and if the likelihood of money laundering or terrorist financing is low. In this case, the verification of identity shall be finished until the completion of the first transaction.

If the client is a legal person or an unincorporated organisation, the due diligence of the legal person or unincorporated company shall also be carried out after the due diligence of the person representing them or acting on their behalf.

Client due diligence measures shall be carried out by the Branch's acting employee in person (except in case of enhanced client due diligence for a client who is not present in person), in the presence of the client/agent/proxy and with the verification of identity documents according to the risk-sensitivity approach.

Client due diligence measures shall not be repeated if:

- the client due diligence measures have already been carried out in relation to the client, agent, proxy, and other authorized representatives in relation to another business relationship or transaction order,
- in relation to this business relationship or transaction order, the identity of the client, agent, proxy, and other authorized representatives has been previously verified and there has been no change in the available data.

The Branch shall be entitled to determine the scope of due diligence measures on a risk-sensitivity basis, and therefore it differentiates between business relationships as follows, also taking into account client due diligence cases:

- client due diligence with reduced data content
- simplified due diligence
- standard client due diligence
- enhanced due diligence.

V.2.2. Verification and verification of identity

In cases listed in point V.1, the client, its agent, the proxy, and other authorised representatives shall be identified, and their identity shall be verified. In doing so, the following information on them, the business relationship, and the transaction shall be recorded on **Schedule 1** (*Identification form*) or on the form(s) of same purpose standardised/issued by the partner insurers:

Identification data in case of natural persons:

1. first and last name,
2. first and last birth name,
3. citizenship,

4. place and date of birth,
5. mother's maiden name,
6. address, if that is not available, place of residence,
7. type and number of identification document.

Identification data in case of legal persons or unincorporated organisations:

1. name, abbreviated name,
2. registered seat, in case of a company with a foreign registered seat, the address of its Hungarian branch if it has one,
3. main activity,
4. the name and positions of its authorised representatives,
5. the data of its agent's for service of process based on which it may be identified,
6. company registration number or in case of other legal persons the number or registration number of the decision on its establishment (registration or incorporation),
7. tax number.

In case of business relationships and transactions, the following data shall be recorded:

1. in case of business relationships, the type, subject, and duration of the contract,
2. in case of transactions, the subject and amount of the order,
3. conditions of performance (place, time, and method).

It shall be mandatory to enquiry about the source of monetary instruments in the following cases:

- if the client or the beneficial owner qualifies as a politically exposed person,
- if the client does not appear in person for the due diligence,
- cash payments of at least EUR 30,000.

In addition to the mandatory cases, if the Branch deems it necessary for any reason (data, facts, or circumstances suggest money laundering or terrorist financing), it shall, on an individual basis, require the client to provide a statement of the source of monetary instruments and may request the presentation of documents on the source of monetary instruments in order to verify such information.

Filling in the identification form shall be the responsibility of the employee in contact with the client, it is forbidden to have the identification form filled out by the client or to hand over the form to the client and request them to return it after filling it in (except in case of enhanced due diligence for a client who does not appear in person).

V.2.3. Transactions subject to management approval

<u>The establishment of a business relationship or the conduction of a transaction shall be subject to management (MLRO) approval:</u>

Based on client risk factors, in the following cases:

a) if, in the course of establishing the business relationship, there is evidence, fact, or circumstance proving that the person behind the service is not actually the person indicated in the contract,
b) if during the establishment of the business relationship the client indicates the conduction of cash transactions exceeding EUR 150,000 per month,
c) if the transaction order exceeds EUR 150,000,
d) if the client is a company, which has a bearer share or whose shareholder is represented by a nominee shareholder,
e) if the client is a company whose ownership structure seems unusual or excessively complex in relation to the nature of the company's business.

Based on the risk factors in connection with the ~~product,~~ service, transaction~~, or used assets~~, in the following cases:

~~a) a business relationship or transaction established with a natural person, who was not present in person, on the basis of a certified copy a document,~~

~~b)~~a) the application of new ~~products~~ services or new business practices substantially different from existing ~~products~~ services or practices, including ~~the application of a new delivery mechanism and~~ new or evolving technologies, for both new and existing ~~products~~services.

Based on the risk factors in connection with the used interface methods, in the following cases:

a) a business relationship or transaction established with a natural person, who was not present in person, on the basis of a certified copy a document.~~;~~

Based on geographical risk factors, in the following cases:

a) if the address or registered seat of the client is in a high-risk third country with strategic deficiencies,
b) if one of the client's owners, that is either a legal person or an unincorporated organisation, has its registered seat in a high risk third country with strategic deficiencies,
c) if the address of the client's beneficial owner, proxy, other authorised representative, or agent is in a high-risk third country with strategic deficiencies.

In all cases, the MLRO of the Branch shall be entitled to grant managerial approval. The request for approval shall be submitted out of turn by the acting employee to the MLRO, in the form of an e-mail, who shall respond to this without delay, but no later than within 2 business days. The written (e-mail) approval shall be kept attached to the client's material. Without approval, a business relationship cannot be established, or a transaction order cannot be conducted. In case of medium high and high risk categories the written approval of the Branch's managing director must also be obtained, the acquisition of which is the responsibility of the MLRO.

Formatted: Justified, Indent: Hanging: 0,02 cm, Space After: 0,55 pt, Line spacing: Multiple 1,03 li

V.2.4. Documents to be submitted

For the verification of identity, the administrator shall require the presentation and check the validity of the following documents:

In case of natural persons:

1. the official document suitable for the verification of a citizen of Qatar and official address card,
2. the 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.

In case of legal persons and unincorporated organisations:

in addition to the presentation of the above-mentioned documents of the person representing them or authorised to act on their behalf, a document, which is not older than thirty days, certifying that

1. the domestic economic organisation has been registered by the QFC-CRO or a registration request has been submitted to that end,
2. in case of other domestic legal persons whose existence is subject to registration by an authority or court, the document of registration,
3. in case of foreign legal persons and unincorporated organizations, the document proving that it has been entered or registered under the law of the country in which it is established.

In case of a request for registration, prior to its submission to the registration authority, the deed of foundation of the legal person or unincorporated organisation shall also be presented.
In this case, the legal person or unincorporated organisation shall document the registration within 30 days thereof and the Branch shall record the registration number or other reference number.

During the verification of the identity the validity of the power of attorney in case of an agent, the validity of the power of disposition in case of an authorised person, and the validity of the power of representation in case of a proxy shall be checked.

In accordance with the risk-sensitivity classification, the person conducting the due diligence shall make a copy of the presented documents. Only the page containing the address of the official address card shall be copied.

The person performing the due diligence cannot be the same as the person subject to the due diligence obligation, in which case another employee of the Branch must take the necessary due diligence measures.

If necessary, the Branch may verify the data concerning identity not only from the presented documents capable of proving the identity but also from the records available in registers containing data for the identification of the person such as search engines/databases on the internet.

V.2.5. Identification of beneficial owners

During the client due diligence, the natural client person shall be present in person and make a written statement on **Schedule 2** (*Customer's beneficial ownership statement*), or on the form(s) of same purpose standardised/issued by the partner insurers in connection with product intermediation if acting in the name or in the interest of the beneficial owner.

The representative of a legal person or an unincorporated organisation client shall declare in writing, on the basis of an accurate and up-to-date record kept by the client, in accordance with **Schedule 3** (*Customer's beneficial ownership*) or on the form(s) of the same purpose standardised/issued by the partner insurers in connection with product intermediation about the beneficial owner of the legal person or unincorporated organisation client.

The declaration shall include the following data on the beneficial owner:

In case of natural person clients:

1. first and last name,
2. first and last birth name,

3. citizenship,
4. place and date of birth,
5. address, if that is not available, place of residence.

In case of legal person or unincorporated organisation clients:

1. first and last name,
2. first and last birth name,
3. citizenship,
4. place and date of birth,
5. address, if that is not available, place of residence,
6. the nature and degree of ownership interest.

The client shall also be required to declare whether the beneficial owner qualifies as a politically exposed person. If the beneficial owner is a politically exposed person, they shall fill in the statement regarding politically exposed persons pursuant to **Schedule 4** (*The statement of politically exposed persons*) or on the form(s) of the same purpose standardised/issued by the partner insurers in connection with product intermediation. The statement shall highlight the basis why the person is considered a politically exposed person.
If there is any doubt as to the identity of the beneficial owner, the client shall be required to make another statement concerning the beneficial owner.

The identity of the beneficial owner may be doubted in the following cases:
- the legal person client changes owners and the background or personal appearance of the new owners (homeless, etc.) are incompatible with their activities, or after the change of ownership the financial activity of the company suddenly changes,
- the ownership structure of the legal person is complex and untransparent, or there are owners registered in high-risk third countries with strategic deficiencies and the „director, representative, manager" etc. person residing in the same country has been nominated as the beneficial owner or the name of the nominated person can be associated with more than one company during an Internet search.

The identity of the beneficial owner shall be verified on the basis of the presented documents, a publicly available register, or any other register from which the Branch is entitled to request data under the law.

Such registers include the QFC-CRO, the company search page of the European e-Justice Portal, company information services on the Internet, registers retrieved by an Internet search, the website of foreign authorities and official bodies, foreign company registers.

In cases where the client has non-natural person owners, when determining the beneficial owner, natural persons who, while maintaining a shareholding or voting right of at least 25% throughout the ownership chain, have real influence on the client's decisions or activities, shall also be taken into account.

V.2.6. Monitoring, enhanced procedure

The business relationship shall be continuously monitored – including the analysis of transactions conducted during the business relationship – in order to determine whether a certain transaction is in accordance with the data on the client that is available to the Branch. Special attention shall be paid to all unusual transactions.

V.2.6.1. Enhanced procedure

Enhanced procedure shall mean the followings:

- gathering further information on
  - the client,
  - the nature of the proposed transaction,
  - the client's monetary instrument and its source,
  - the purpose of the proposed or conducted transaction,
- priority examination of the number and timing of business relationships with the client, and
- selection of a transaction for further investigation.

When selecting a transaction for further investigation, a transaction of at least EUR 30,000 shall be selected. If the selected transaction is a cash payment, information on the source of the monetary instrument shall also be obtained.

The continuous monitoring of a business relationship shall be carried out as an enhanced procedure in the following cases:

- in case of a politically exposed person,
- in case of a business relationship or transaction with a natural person client not being present in person based on a certified copy of a document;
- in case of a non-governmental or municipally owned non-profit economic organisation;
- in case of a client whose address or registered seat is in a high risk third country with strategic deficiencies;
- in case of a beneficial owner whose address is in a high risk third country with strategic deficiencies;
- in case of a client that is a company, which has bearer shares or whose shareholder is represented by a nominee shareholder;
- in case of a client that is a company with unusual or excessively complex ownership structure considering the nature of the company's business activity.

V.2.7. Cases of termination of business relationships

A business relationship shall not be established, an existing business relationship shall be terminated, and a transaction shall not be conducted if the result of the client due diligence required by AML/CFTR is not fully available to the Branch, that is if the client due diligence cannot be performed comprehensively, due to:

- the client refusing to make a statement of the beneficial owner,
- there still being doubts as to the identity of the beneficial owner even after a repeated (written) statement by the client,
- there still being doubts following the client's repeated (written statement – concerning the beneficial owner,
- the source of monetary instruments not being clarified to the satisfaction of the Branch.

Doubts concerning the authenticity or accuracy of client identification data may arise due to, among others:

- certain elements and the visual composition of the identity card or driving license card not complying with the requirements of the issuing authority,
- individual security features – in particular, the hologram, the kinegram or other equivalent security features – being unrecognizable or damaged,
- the ID number of the of the identity card or driving license card being unrecognisable or damaged,

- the client's face not matching the portrait on the identity card or driving license card presented by them,
- the data on the identity card or driving license card not logically corresponding to the data available on the client.

V.3. Client due diligence with reduced data content

The Branch shall use due diligence with reduced data content in only the following two types cases:
1. regular business connection or/and series of related transaction, or
2. client due diligence performed by other service providers.

V.3.1. Client due diligence in the case of regular business connection or/and series of related transaction

In order to record a series of related transactions, the following data shall be recorded when conducting a transaction order, the value of which exceeds EUR 1000, but is less than EUR 10,000:

In case of a natural person client:
- first and last name,
- place and date of birth,
- the subject and amount of the transaction order.

In case of legal person or unincorporated organisation client:
- name and abbreviated name,
- registered seat, in case of a company with a foreign registered seat, the address of its Hungarian branch if it has one,
- the subject and amount of the transaction order.

It is not compulsory to present documents suitable for proving one's identity, nor to make a copy of them, but in order to verify one's identity, the presentation of documents may be requested – taking into account individual circumstances.

V.3.2. Client due diligence in the case of performed by other service providers

The AML/CFTR allows the acceptance of the result of a client due diligence performed by another service provider, however, the responsibility for meeting the client due diligence requirements rests with the service provider accepting the result of the client due diligence performed by another service provider. The result of a client due diligence performed by another service provider may be accepted with the consent of the client, since the service provider shall only be entitled to make the data required for the client due diligence available to another service provider with the consent of the client concerned.

The Branch accepts the results of client due diligences performed by other service providers applying the AML/CFTR.

V.4. Simplified client due diligence as per Part 4.5 of the AML/CFTR

The following are not exhaustive, and must extend, but does not limit, the meaning of these rules or particular provisions of these rules to which relates, as per Part 4.4 of the AML/CFTR.

The Branch shall use simplified due diligence in the following cases:

Low and medium low risk factors:

A. Client risk factors:

Transactions shall mean low-risk business relationships where the client is one of the following entities/organisations:

- service providers with a registered seat in the State of Qatar that pursue the following activities: credit institutions, financial service providers (financial enterprises, payment institutions pursuing money processing activities, electronic money institutions, issuers of credit tokens, currency exchange offices, insurers, multiple agents and brokers, as well as multiple special services intermediaries and brokers, investment firms, commodity dealers, investment fund managers, and market operators), institutions for occupational retirement provision, voluntary mutual insurance funds, international money order withdrawers and deliverers. In addition, service providers with a registered seat in another country that are carrying out the above activities, provided, that they are subject to requirements equivalent to those provided for by the law and are supervised as regards to their compliance with such,
- service providers with a registered seat in the European Union that pursue the following activities: credit institutions, financial service providers (financial enterprises, payment institutions pursuing money processing activities, electronic money institutions, issuers of credit tokens, currency exchange offices, insurers, multiple agents and brokers, as well as multiple special services intermediaries and brokers, investment firms, commodity dealers, investment fund managers, and market operators), institutions for occupational retirement provision, voluntary mutual insurance funds, international money order withdrawers and deliverers. In addition, service providers with a registered seat in another country that are carrying out the above activities, provided, that they are subject to requirements equivalent to those provided for by the law and are supervised as regards to their compliance with such,
- supervisory body: Supervisory Body, chamber of auditors, regional bar association/regional association of notaries, authority for trade and commerce, authority functioning as a financial intelligence unit,
- local governments, budgetary institutions of local governments, central governmental entity,
- institutions of the European Union, (European Parliament, Council of the European Union, European Commission, Court of Justice of the European Union, European Court of Auditors), European Economic and Social Committee, European Committee of Regions, European Central Bank, European Investment Bank, or any other body or institution of the European Union,
- a company whose securities are admitted to trading on a regulated market in one or more Member State (Plc.) or a company in another country which is subject to disclosure requirements under community law,
- administrative authorities or majority-state-owned economic companies,
- clients residing in low-risk geographical areas as defined in point C.

B. Risk factors related to ~~products,~~ services~~, transactions or service channels~~:

- simple agency contracts such as representation in a registration procedure,
- conclusion of an agency contract with a value not exceeding EUR 1000.

C. Interface risk factors:

- face-to-face business relationships transactions and service,
- reliable technologies used for provision of services that are regarded as secure under applicable law.

Formatted: Font: Bold

Formatted: Justified, Indent: Hanging: 0,5 cm, Space After: 0,55 pt, Line spacing: Multiple 1,03 li, Bulleted + Level: 2 + Aligned at: 1,51 cm + Indent at: 1,51 cm

Formatted: Font: Not Bold

Formatted: No bullets or numbering

~~C.~~D. **Geographical risk factors:**

- Member States of the European Union;
- countries with effective systems for countering money laundering and terrorist financing,
- countries with at least low levels of corruption or other criminal offenses, based at least on the World Bank's Governance Indicators index and on other sources, in particular, evaluation reports adopted by international organizations;
- countries whose anti-money laundering and anti-terrorist financing standards are in line with the revised FATF recommendations and are effectively applying them.

In case of simplified client due diligence the Branch – for the purposes of identifying the client, or business relationship or transaction order for the prevention and countering of money laundering and terrorist financing – shall be obliged to continuously monitor the business relationship in accordance with the legal provisions governing its activities – including the analyses of transactions conducted during the duration of the business relationship –, in order to determine whether the given transaction is in accordance with the data on the client available to the service provider under the law; furthermore, it shall be obliged to record the identification data specified in point V.2.2 (identification data in case of natural persons and legal person, as well as unincorporated organisation clients) and shall request the presentation of the documents specified in point V.2.4 for the verification of identity.

V.5. Standard client due diligence as per Part 4.3 of the AML/CFTR

The following are not exhaustive, and must extend, but does not limit, the meaning of these rules or particular provisions of these rules to which relates, as per Part 4.4 of the AML/CFTR.

The Branch shall apply complete client due diligence in the following cases:

Medium ~~R~~risk factors:

A. Risk factors related to ~~products,~~ services~~, transactions or service channels~~:

- conduction of a transaction order, if its amount – either as a single transaction or a series of related transactions – is at least EUR 10,000.

The Branch shall be obliged to record the data specified in point V.2.2. The client shall be obliged to make a statement of regarding the beneficial owner as defined in V.2.5.
Each natural person client shall be obliged to make a written statement in person as to whether the client and its beneficial owner qualify as a politically exposed person and, if so, in what capacity, at the time of establishing the business relationship or no later than prior to the conduction of the transaction order, if they have not previously made a statement. If the client or its beneficial owner qualifies as a politically exposed person, it shall already be covered by the enhanced client due diligence and the measures specified for the enhanced client due diligence shall be applied.

The Branch shall request, verify, and make a copy of the documents specified in point V.2.4 for the verification of their identity.

In addition to the due diligence of the legal person or the unincorporated organisation, the Branch shall be obliged to perform the due diligence of the person representing or acting on behalf of the legal person or unincorporated

organisation (representative), and therefore the representative's identity documents shall be presented, verified, and made a copy of.

In case of complete client due diligence the Branch – for the purposes of identifying the client, or business relationship or transaction order for the prevention and countering of money laundering and terrorist financing – shall be obliged to continuously monitor the business relationship in accordance with the legal provisions governing its activities – including the analyses of transactions conducted during the duration of the business relationship –, in order to determine whether the given transaction is in accordance with the data on the client available to the service provider under the law.

V.6. Enhanced client due diligence as per Part 4.4 of the AML/CFTR

The following are not exhaustive, and must extend, but does not limit, the meaning of these rules or particular provisions of these rules to which relates, as per Part 4.4 of the AML/CFTR.

The Branch shall apply enhanced client due diligence in the following cases:

Medium high to ~~H~~high risk factors:

A. Client risk factors:

- the client or its beneficial owner is a politically exposed person,
- a non-state, or -municipally owned non-profit economic company,
- a company that has a bearer share or whose shareholder is represented by a shareholder nominee,
- a company whose ownership structure seems unusual or excessively complex considering the nature of the company's business activity,
- the business relationship takes place under unusual circumstances,
- clients who reside in high-risk geographical areas as defined in point C,
- trusts,
- enterprises whose degree of money processing activities is considered significant by the supervisory authorities.

B. Risk factors related to services ~~products, services, transactions or service channels~~:

- ~~client's lack of personal attendance,~~
- ~~products or~~ services or transactions for which the client has not been identified,
- payments from third parties that are unknown or not involved in the business relationship or transaction,
- the offering and application of new ~~products~~ services or new business practices substantially different from existing ~~products~~ services or practices, including ~~the application of a new delivery mechanism and~~ new or evolving technologies, for both new and existing ~~products~~services.

C. Interface risk factors:

- client's lack of personal attendance,
- lack of reliable technologies used for provision of services that are regarded as secure under applicable law.

D. Geographical risk factors:

Formatted: Indent: Left: 0,5 cm, Hanging: 0,5 cm, Bulleted + Level: 1 + Aligned at: 1,51 cm + Indent at: 1,51 cm

Formatted: Font: Not Bold

- the address of the legal person's or unincorporated organisation's beneficial owner is in a high-risk third country or geographical area with strategic deficiencies,
- countries that do not have effective systems in place to combat money laundering and terrorist financing;
- countries with high levels of corruption or other criminal offenses – based at least on the World Bank's Governance Indicators index and on other sources, in particular, evaluation reports adopted by international organizations,
- countries subject to sanctions imposed by the European Union or the UNSC,
- countries that are known to finance or support terrorist activities or that have known terrorist organizations operating in their territory.

In the above cases, the following enhanced client due diligence measures shall be taken in addition to the complete client due diligence measures:

V.6.1. Clients not being present in person

For the purposes of identification and the verification of identity documents, a certified copy of the documents containing the identification data shall be requested in all cases where the client, proxy, representative, or agent did not show in person for the purposes of their identification and the verification of their identity.

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

- it has been authenticated by a notary public or the Hungarian foreign representation authority pursuant to provisions of Act XLI of 1991 on Notaries concerning the certification of the authentication of a copy, or
- the copy was made by the authority of the state where the document was issued, which is authorized to make a certified copy, and – unless otherwise provided by an international treaty – the Hungarian foreign representation authority has authenticated the signature and stamp of this authority on the copy.

In case of a client that has not been present in person, the establishment of a business relationship and the conduction of a transaction order may only take place after the approval of the managing director of the Branch. The request for approval shall be submitted out of turn by the acting consultant to the managing director, in the form of an e-mail, who shall respond to this without delay, but no later than within 2 business days. The written (e-mail) approval shall be kept and archived attached to the client's material. Without approval, a business relationship cannot be established, or a transaction order cannot be conducted.

The Branch shall only accept documents in English without a translation. The Branch shall only accept certified translations of foreign language documents.

V.6.2. Due diligence of politically exposed persons

The natural person client shall be obliged to make a written statement in person according to **Schedule 5** (*Politically exposed person's statement*) or on the form(s) of same purpose standardised/issued by the partner insurers in connection with product intermediation as to whether they qualify as a politically exposed person.

It is recommended that the statement is verified on the basis of publicly available information on the Internet.

If the person making the statement qualifies as a politically exposed person, the statement shall also include the point on the basis of which they qualify as such. The statement shall also include information on the source of monetary instruments.

In the case of a key public actor, the establishment of a business relationship and the conduction of a transaction order may take place only after the approval of the managing director of the Branch. The request for approval shall be submitted out of turn by the acting consultant to the managing director, in the form of an e-mail, who shall respond to this without delay, but no later than within 2 business days. The written (e-mail) approval shall be kept and archived attached to the client's material. Without approval, a business relationship cannot be established, or a transaction order cannot be conducted.

The monitoring of a business relationship with a politically exposed person shall be carried out in an enhanced procedure (point V.2.6.1.)

The client's statement about the quality of their politically exposed status may not be omitted.

V.6.3. In every other case

In cases not covered by points V.4.1.-V.4.2., an enhanced procedure shall be performed (point V.2.6.1.).

V.7. The use of an audited electronic communication device

The Branch shall use an audited electronic communication device.

V.8. Internal risk assessment

The Branch shall prepare its internal risk assessment as part of this Policy, based on the AML/CTFR and the potential provisions of the supervisory authority. Risk management should be reviewed annually and updated as necessary. Based on the performed risk assessment, appropriate risk management measures shall be implemented to mitigate the identified risks. The risk assessment shall be approved by the managing director.

The Branch identifies and evaluates risk factors related to the nature and amount of the business relationship or transaction order, client, ~~product,~~ service, geographical area and used ~~asset~~ interface methods to identify and assess its risks.

Formatted: Justified

The Branch shall consider the following when identifying risk factors:

- recommendations issued by the supervisory authority,
- information disclosed by the supervisory authority and documents generated and disclosed over the course of the supervisory authority's proceedings.

In identifying risk factors, the Branch may take into account, in particular, information from:

- the civil society,
- an assessment of the adequacy and effectiveness of the anti-money laundering and anti-terrorist financing system as well as the anti-corruption and taxation system of the evaluated Member State,
- public sources, and
- scientific institutions.

The Branch is not exposed to the money laundering and terrorist financing risks of another state or country as, amongst others

- it does not have a business relationship with another state, or person registered or residing in another country,
- it is not a member of a financial group established in another Member State or in a third country,
- it does not maintain any relationship with any other state or country that indicates that Branch is exposed to that country's money laundering and terrorist financing risks.

V.8.1. Classification of clients into risk categories

Clients shall be classified into risk categories for money laundering and terrorist financing, for which information on the purpose and intended nature of the business relationship must be obtained. The Branch shall decide on the client's risk rating in cases not regulated by the law. Clients, ~~products,~~ services, ~~assets~~ used interface methods, and geographic risk factors ~~risks~~ (and other qualitative risk factors as may be determined internally) ~~should be categorized based on risk factors~~shall be taken into consideration and evaluated during the classification process.

For the purposes of client classification the Branch uses the following multi-level risk category structure (which is further discussed in the Branch's internal risk assessment manual attached hereto as Schedule 11):

1. Low risk category
2. Low medium risk category
3. Medium risk category
4. Medium high risk category
5. High risk category

V.8.2. Aspects to be taken into account for internal risk assessments, risk factors:

- the Branch's ownership and corporate structure,
- the complexity and transparency of the organisation and structure of the Branch,
- the reputation and integrity of the Branch's senior management, members of its governing body, and its owner with qualified interest,
- the nature and complexity of the ~~product or~~ service offered, the activity, and the transaction conducted,
- the means used, including the provision of service free of charge, and the use of an agent or intermediary,
- the types of clients served,
- the geographical area of the Branch's business, in particular if that is carried out in a high risk third country with strategic deficiencies, or if the country of origin of a significant proportion of its clients is a high-risk third country with strategic deficiencies,
- the quality of the Branch's internal management solution and structure, including the effectiveness of the internal audit and compliance function, compliance with legal requirements relating to the prevention and countering of money laundering and terrorist financing, and the effectiveness of its internal risk assessment,
- the prevailing company culture of the service provider, in particular its compliance and transparency culture,
- experience of cooperating with authorities,
- other prudential aspects.

Factors (non-exhaustive list) to be considered when classifying a client into a risk category (please also see the stages for classification in clause II.3 of the internal risk assessment manual attached hereto as Schedule 11 (with special attention to the RAG matrix and the detailed explanation of each risk category)):

Low and low medium risk factors:

- Client risk factors:
  - companies whose securities are listed on a stock exchange and are subject to disclosure requirements, which ensure the adequate transparency of the beneficial ownership;
  - administrative authorities or a majority-state-owned economic company;
  - clients residing in low-risk geographical areas as defined in point on the geographical risk factors.
- Risk factors related to ~~products,~~the services~~, transactions or service channels~~ provided by the Branch:
  - s~~S~~ervices in connection to which the money laundering and terrorist financing risk is addressed through other measures like restrictions on electronic monetary instruments or the transparency of ownership (for example certain types of electronic money).
- Interface risk factors:
  - the transaction/service involves face-to-face business relationships or investment orders/transactions, or in case od non-face-to-face transactions the appropriate safeguards (that are deemed acceptable by applicable law) are in place (e.g.: diligent electronic identification process which meets the conditions set out in applicable law, like electronic signatures and electronic ID cards)
- Geographical risk factors:
  - Member States of the European Union;
  - third countries with effective systems for countering money laundering and terrorist financing;
  - countries with at low levels of corruption or other criminal offenses – based at least on the World Bank's Governance Indicators index and on other sources, in particular evaluation reports adopted by international organizations;
  - countries whose anti-money laundering and anti-terrorist financing standards are in line with the revised FATF recommendations and are effectively applying them.

Medium risk factors:

- Client risk factors:
  - clients with sources of income that are not employment-based or are not from a regular known source;
  - clients that are engaged in cash sensitive businesses.
- Risk factors related to the services provided by the Branch:
  - one-off transactions (or transactions that do not necessarily fit with the client's overall commercial behaviour)
- Interface risk factors:
  - participation of one or more intermediaries in a transaction
  - moderately reliable means of communication and instructions (e.g. videocall)
- Geographical risk factors:
  - third countries with moderately effective systems for countering money laundering and terrorist financing;
  - countries with medium levels of corruption or other criminal offenses – based at least on the World Bank's Governance Indicators index and on other sources, in particular evaluation reports adopted by international organizations.

Formatted: Underline

Formatted: Normal, Indent: Left: 2,25 cm, Hanging: 1 cm, Tab stops: 3,25 cm, Left

Formatted: Indent: Left: 2,25 cm

Formatted: Indent: Left: 2,25 cm, Space After: 0,55 pt

Medium high and ~~H~~high risk factors:

- Client risk factors
  - the business relationship takes place under unusual circumstances;
  - clients whose address is in high-risk geographical areas as defined in point 3;
  - trusts;
  - companies that have bearer shares or whose shareholder is represented by a nominee shareholder;
  - enterprises whose degree of money processing activities is considered significant by the supervisory authorities;
  - companies whose ownership structures seem unusual or excessively complex considering the nature of the company's business activity;
- Risk factors related to ~~products~~ the~~,~~ services~~, transactions or delivery channels~~ provided by the Branch:
  - ~~products~~ services or transactions in case of which the client has not been identified;
  - ~~non-personal business relationships or transactions without certain security precautions – such as the use of electronic signatures or electronic identity cards;~~
  - payments from third parties that are unknown or not involved in the business relationship or transaction;
  - the application of new ~~products or new~~ services, business practices substantially different from existing ~~products or~~ practices~~, including the application of a new delivery mechanism and new or evolving technologies, for both new and existing products~~.
- Interface risk factors:
  - the transaction/service involves non-face-to-face business relationships or investment orders/transactions without any safeguards or verification possibilities (such as an electronic identification process compliant with applicable laws)
- Geographical risk factors:
  - countries that do not have effective systems in place to combat money laundering and terrorist financing;
  - countries with high levels of corruption or other criminal offenses – based at least on the World Bank's Governance Indicators index and on other sources, in particular evaluation reports adopted by international organizations;
  - countries subject to sanctions imposed by the European Union or the UNSC;
  - countries that are known to finance or support terrorist activities or that have known terrorist organizations operating in their territory.

The Branch shall assess the impact of the risk factors listed above on the Branch.

The risk-based approach aims to identify and reduce internal risks related to money laundering and terrorist financing by developing appropriate and effective measures.

~~Risk-based analysis as per Part 3 of the AML/CFTR regarding the risk assessment process, and as per Appendix I, II and III of the "Guidance on Risk-Based Approach" document.~~

The risk-based analysis shall be performed in relation to the Branch for the following risk categories:

1. ~~Product~~ Service risk

Formatted: Indent: Left: 1,25 cm, Hanging: 1 cm

Formatted: Indent: Left: 2,25 cm, Hanging: 1 cm, Tab stops: 3,25 cm, Left

Formatted: Left, Indent: First line: 0 cm, Space After: 0 pt, Line spacing: Multiple 1,08 li

Based on certain characteristics, some ~~products~~ services are much more attractive and suitable for money laundering and terrorist financing offenses.

2. ~~Sales channel~~Interface risk

There are various risks involved in the way the service is ~~sold~~provided (e.g. used technologies) and in the mechanisms through which business relationships with a client are started or conducted. ~~N~~For example, non-personal transactions ~~sales-like~~ where instructions are given online ~~sales or sales~~or over the phone pose a greater risk of money laundering and terrorist financing because they increase the risk of the client using a fake identity. ~~The Branch only accepts orders based on recommendations from previous clients and relationships of trust between Branch and its clients. It does not use a marketing tool to promote their activity. Separate sales, low-risk client acquisition at professional conferences.~~

~~3. Country risk~~

~~It represents the risk of the country and region in which the Branch has its registered seat.~~

~~4.~~3. Geographical (jurisdiction) risk

It represents the risk related to the client's place of residence/incorporation or citizenship or where the client conducts business or has assets. (As part of the jurisdiction risk, the Branch may also take into consideration the possible risk that could arise from the fact that the services are provided and the activities are carried out in Qatar, as and if applicable under the given circumstances.)

~~5.~~4. Client risk

It represents the risks associated with the client profile and the expected behaviour of the client. The risk increases if the client does not seem to be acting in their own interest (for example, they make an economically unjustified decision like requesting the termination of the contract without an obvious reason resulting in additional costs being charged), or if their actions are inconsistent with their business practices.

~~6. Interface risk~~

~~By definition of applicable QFC AML/CFT legislation, it relates to the risks posed by the mechanisms through which business relationships with a firm are started or conducted.~~

~~7. Jurisdiction risk~~

~~It refers to the risk that arises when operating in a foreign jurisdiction. This risk can come by simply doing business or carrying out financial transaction in another country.~~

The ~~designated person~~MLRO shall perform, review, update and document the risk assessment at least annually or as required (e.g. an external effect changes the nature of the risk or a new type of money laundering and terrorist financing risk arises, etc.), while assessing a risk rating by each individual activity/service conducted as well as an overall risk rating. Based on the performed risk assessment, appropriate risk management measures shall be implemented to mitigate the identified risks. The risk assessment shall be approved by the managing director.

V.8.3. Risk management

Following the risk assessment, the necessary measures shall be identified to appropriately address the risks related to money laundering and terrorist financing. There are two possible ways to do this:

a) Reducing the risk
   - performing client due diligence measures on a risk-sensitivity basis,
   - ex-ante application of the sanction list filtering system to check if the natural or legal person is not in the database,
   - further measures to explore the possible relationship of a given client or contract with a sanctioned country,
   - continuous monitoring of the client, contract, and transactions,
   - obtaining additional documents in connection with higher risk contracts,
   - preparing process descriptions and internal rules of procedures for dealing with money laundering and terrorist financing risks,
   - teaching the recognition of circumstances that increase money laundering and terrorist financing risk, as well as suspicious behaviour.

b) Elimination/avoidance of risk

The Branch may decide that the establishment of a business relationship infers too high or disproportionate risk to its potential financial benefit. For example, the Branch may decide not to enter into a contract due to certain circumstances (e.g. capital coming from certain countries or unregulated foundations, etc.).

The Branch aims to avoid/ex-ante mitigate client risks by primarily accepting new clients based on the recommendations from previous and reliable clients and aims to establish a restricted client portfolio with relationship based on trust between the Branch and its clients. The Branch does not use a marketing tool to promote its activity, low-risk client acquisition will take place at professional conferences.

The branch may change its internal risk assessment out of turn if:

- an external effect changes the nature of the risk,
- a new type of money laundering and terrorist financing risk arises,
- the finding of the supervisory authority includes such a measure,
- it comes from the Branch's own risk mitigation measures,
- new information arises regarding the owner of the Branch, the persons performing the main functions, or its organization, and
- in all other cases where the Branch has good reason to believe that the information on which the risk assessment is based is no longer applicable.

VI. REPORTING OBLIGATION AS PER Chapter 5 OF THE AML/CFTR

The employees shall, without delay, report any information, fact, or circumstance indicating:

- money laundering,
- terrorist financing, or
- that a specific property is derived from criminal activity,

to the designated person as set out in **Schedule 6** (*Reporting of information, fact or circumstance indicating the occurrence of money laundering and terrorist financing*).

The Branch has information on the client's financial situation, payment practices, including payment discipline, through the client's existing contracts and client relationship. Due to the organized nature of money laundering, concluding a contract by encouraging payment in cash is not less suspicious than paying by electronic means if it is unusual considering the client's known financial situation and insurances. Thus, any transaction that does not

fit into the client's account history, known business habits and practices can be an unusual transaction. **Schedule 10** (*Typical behaviours of money laundering and terrorist financing)* of this Policy describes the typical criminal behaviours, the occurrence of which raises a suspicion of money laundering, terrorist financing, or that a specific property is derived from criminal activity.

The report shall contain:

- data and information the Branch has recorded based on the customer due diligence measures,
- detailed description of the information, fact, or circumstance on which the reporting is based, and
- documents supporting the information, fact, or circumstance relevant for the reporting, if available.

The report shall be submitted to the designated person electronically to the electronic address set out in Part 3, point X.1 of the Policy, or in printed form in person. Upon receipt of the report, the designated person shall acknowledge receipt of the report to the reporting party. The designated person shall keep an internal record of the received reports. Reports received by e-mail shall be printed by the designated person. The designated person shall keep the reports received by him in a paper form for the period specified in the relevant legislation. In addition to the designated person, the managing director is also entitled to access the data specified in the reports.

The report shall be examined for the transaction conducted or to be conducted and for the transaction initiated but not conducted by the client and if the performance of the client due diligence measures has failed.

By the decision of the MLRO, a transaction cannot be conducted until the report is forwarded to the FIU. If non-execution of the transaction is not possible or the execution of the report prior to the execution of the transaction would jeopardize the monitoring of the beneficiary, the designated person shall forward the report after the execution of the transaction.

VI.1. Content of the report and applicable rules

- name and data of the Branch, as well as the name, work address and phone number of the designated person,
- identification data of the client,
- description of the information, fact, or circumstance on which the report is based,
- actions taken by the Branch,
- date of the report.

The available documents proving the existence of the information, fact or circumstance indicating money laundering and terrorist financing shall be attached to the report.

The reporting employee is responsible for completing the report form and submitting it to the designated person.

By decision of the MLRO, a reports must be submitted to the FIU whose, contact details are set out in **Schedule 7** to this Policy (*Contact details of the FIU*). The designated person shall examine the report received without any delay and, if he deems it necessary to make an official notification, he shall make the notification after filling out the electronic form required for such official notification. The designated person shall forward the report thorugh the FIU-website (http://www.qfiu.gov.qa), on behalf of the Branch in the form of a protected electronic message, upon the receipt of which the financial information unit immediately notifies the Branch in the form of an electronic message.

The FIU may request the supplementation of the information, facts, and circumstances indicating money laundering and terrorist financing, which request must be complied with.

VI.1.1. Suspension of the transaction

The suspension of the transaction takes place in order to enable the FIU to take immediate action if information, fact, or circumstance indicating money laundering or terrorist financing arise in connection with a transaction. In this case, the designated person is obliged to notify the FIU without delay.

When making the notification, the designated person, or, if he is prevented from doing so, the person appointed by him, may inform the FIU via phone call about the information, fact or circumstance on which the suspension is based so that they can agree on the information to be provided to the client and that the FIU's may give instructions as to the implementation of the suspension. In case the FIU does not provide any instructions for informing the client, a technical error may be primarily invoked. Under no circumstances may the information indicate the fact of the transaction's suspension and the reason for the suspension. The managing director of the Branch and the designated person are entitled to access the suspension data.

Suspending a transaction may be conducted by the suspension of all other transactions with respect to services provided to the client involving transactions to the debit of the client's assets. Such case shall be brought to the attention of the FIU in the submitted report.

A suspended transaction order shall be conducted if, based on the notification of the FIU, the transaction order can be conducted during the period of suspension, or if 4 business days have elapsed after the suspension of the transaction without notifying the FIU.

Execution of transactions shall be suspended if the FIU sends a notification in writing in connection with the transaction or of any data, fact, or circumstance relevant for reporting in relation to the client.

The FIU is entitled to extend the period of investigation once by an additional 3 business days, in which case it will notify the Branch.

The FIU will send a written notification within 4 business days, if

- it extends the investigation,
- the transaction can be conducted before the investigation of the FIU is completed.

The designated person will only include those Branch employees in the suspension procedure whose involvement is absolutely necessary.

VI.1.2. Immunity

Disclosure of information by the reporting person or the Branch acting in good faith shall not invoke civil or criminal liability even in circumstances where the report ultimately proves to be unfounded, or the suspended transaction may be carried out afterwards.

VI.2. Prohibition of disclosure and tipping off

No disclosure shall be made to the client or to other third persons, organisations

- of the fact that a report has been filed, on the provision of information upon request, the contents of such information,
- on the suspension of the transaction,
- on the identity of the reporting person, or
- of whether any criminal procedure has been instituted against the client.

No tipping-off shall be made to the client or to other third persons, organisations as per Part 5.2 of the AML/CFTR.

The filing of the report, the contents thereof, and the identity of the person filing the report shall remain confidential. Such limitation shall not include any disclosure to the supervisory authority by the reporting person, or the transmission of information at the request of the FIU if it requests information in order to carry out its statutory task.

VII. INTERNAL CONTROL AND INFORMATION SYSTEM

In order to prevent a business relationship or transaction that enables or implements money laundering or terrorist financing, the Branch operates internal control procedures and an information system, which promote client due diligence, the implementation of reporting, and record-keeping. Branch uses its best efforts to operate the screening system. The number of the Branch's clients is not significant, therefore it performs manual screening.

The Branch operates a screening system under which the detecting person informs the designated person of the following cases in particular:

- the involvement of a politically exposed person or a foreign person arises during the recording of the data sheets;
- if the client, the client's agent, proxy, or other authorized representative did not appear in person for the purpose of identification and verification of identity;
- if the client is from a high-risk third country with strategic deficiencies;
- the client is not a state owned or municipally owned non-profit organisation;
- the beneficial owner of the client is domiciled in a high-risk third country with strategic deficiencies;
- the client is a company that has a bearer share or whose shareholder is represented by a shareholder's proxy;
- if the client is a company whose ownership structure appears unusual or excessively complex considering the nature of the company's business;
- the client has made a doubtful statement as to the source of the funds;
- other suspicious information arose during the monitoring activity;
- other unusual transactions implying money laundering and terrorist financing.

All of clients and transactions must be screened:

- cash payment of EUR 70,000 or more for a natural person client,
- cash payment of EUR 140,000 or more to legal entity clients and unincorporated organisation clients,
- cash payment of EUR 70,000 or more to a natural person client,
- cash payment of EUR 140,000 or more to legal entity clients and unincorporated organisation clients, and
- a transaction of EUR 14,000 or more initiated from or transferred to a high-risk third country with strategic deficiencies.

The Branch constantly revises the screening criteria. The Branch may determine additional screening criteria based on the national and internal risk assessment.

The Branch shall continuously perform screening for money laundering and terrorist financing. The analysis and evaluation of the screened client or transaction for money laundering and terrorist financing should be carried out without delay. The process of analysing and evaluating the screened client or transaction is documented by the Branch in such a way that the result of the measure implemented by the Branch's employee and the decision made based on it may subsequently be reconstructed.

The Branch ensures that the Branch can fully and promptly handle any requests from the FIU, the supervisory authority, or law enforcement agencies.

The Branch ensures that the internal control procedures and information system is capable of sorting the business relationships based on

- personal data,
- account number,
- client number,
- transaction type, or
- amount limit.

The internal control and information system is capable of registering the data recorded in it for retrieval within the period specified in the AML/CFTR.

VII.1. Abuse reporting system

The Branch ensures that its employee can send anonymous report in the event of a breach of the AML / CFTR provisions by the Branch, for which purpose it operates an anonymous abuse reporting system. An employee of the Branch may send an anonymous letter to the registered seat of the Branch at all times addressed to the designated person.

A report may be made by an employee who is aware of the fact that the Branch is violating or has violated the provisions of the AML / CFTR. The report must be examined within 30 days, which does not include the date on which the report was made. The person making and affected by the report shall not take part in the investigation of the report. The managing director of the Branch, the designated person, and the administrative team leader are eligible to participate in the investigation.

Depending on the results of the investigation:

- if any information, fact, or circumstance arises, which indicates money laundering, terrorist financing or that a specific property is derived from criminal activity, the designated person shall immediately notify the FIU,
- if there is a suspicion of a criminal offense, the managing director of the Branch shall immediately report it to the investigating authority with invested authority and competence,
- in addition to the above, if the Branch finds a violation of the AML / CFTR or of the regulations of any supervisory authority, the designated person shall immediately notify the supervisory authority.

Once a report has been made, it may not be accessed by anyone other than the person involved in the report or its investigation. To this end, the Branch keeps the information, facts, and documents related to the report in a separate register / file, which can only be accessed by the authorised persons.

PART 2: PROVISIONS FOR THE IMPLEMENTATION OF THE UNSC RESOLUTIONS

VIII. THE PURPOSE OF THE FINANCIAL AND PROPRIETARY RESTRICTIVE MEASURES ORDERED BY THE UNSC

The purpose of this policy is to

- freeze,
- prohibit the active accessibility of

the economic resources and financial assets of the subject of the financial and proprietary restrictive measures.

The implementation of the financial and proprietary restrictive measures regulated herein is aimed at the implementation of the proprietary and financial restrictive measures ordered by a resolution of the UNSC.

IX. IMPLEMENTATION OF THE FINANCIAL AND PROPRIETARY RESTRICTIVE MEASURES

The Branch continuously monitors the issuance of and the subsequent amendments to UNSC resolutions imposing financial and proprietary restrictive measures. The Branch takes into account these UNSC resolutions ordering financial and proprietary restrictive measures.

IX.1. Screening-monitoring system

The Branch operates a screening system capable of ensuring the prompt and entire implementation of UNSC resolutions imposing financial and proprietary restrictive measures. The Branch operates an automatic screening system to ensure the prompt implementation of UNSCRs imposing financial and proprietary restrictions. Branch will do everything in its power to operate the screening system.

The Branch is constantly screening for the financial and proprietary restrictive measures imposed by the UNSC. It shall be checked whether the client is on one of the sanctions lists at least when establishing a business relationship; the entire client base shall be checked upon the change of the sanction lists.

Verification of the contractor must be carried out during the contracting process.
The verification of the client (whether a natural or a legal person) should be performed primarily on the basis of the name / title recorded in the system, by comparison with the names in the database. In order to achieve a more accurate result, the date of birth, gender, and citizenship may be added as additional filtering criteria, provided that such data have been recorded in the systems. Results obtained accordingly from the comparison performed on the basis of the above data shall be considered suspicious if the match rate reaches or exceeds 92%.

In the event of a suspicious hit, the contracting process is suspended and investigated by the designated person. The purpose of the further investigation is to transmit only those hits that are in fact suspicious, out of all those that are automatically filtered out by the IT system based solely on the names or other existing data matching, as listed above.

If the data recorded in the system is incomplete or inaccurate / incorrect, without which a decision on the merits cannot be made in the given case, the necessary measures shall be taken in order to collect and clarify the relevant data.

With respect to suspicious hits, the following tests must be performed by the designated person:
- verification of the available documents,
- verification of the data recorded in the IT systems,
- checking additional publicly available databases (e.g. QFC-CRO),
- checking other sources (e.g. internet).

If after conducting the above investigation the suspicious hit is considered a false hit, then the designated person will indicate this, after which the business relationship may be established.
If, following the above investigation, the suspicious hit is considered a real hit, the designated person shall arrange for the hit to be reported to the authority in accordance with point IX.2.

The Branch will retain the data generated during the performance of the screenings for eight years from the time the screening is performed.

The Branch does not screen based on other lists in addition to the required lists.

The contact details of the lists relevant to the prevention and countering of terrorist financing are set out in **Schedule 8** to this Policy (*Contact details of the lists relevant to the prevention and countering of money laundering and terrorist financing and compliance with embargo restrictions*).

IX.2. Reporting obligation based on the application of these rules

The designated person shall immediately notify the FIU (**Schedule 9**) of any information, fact, or circumstance indicating that the subject of the financial and proprietary restrictive measures has funds or economic resources in the territory of Hungary that are subject to the financial and proprietary restrictive measures.

The notification provisions of the AML/CFTR shall apply mutatis mutandis to such notification.

The designated person is responsible for completing the notification form and submitting it to the FIU.

The FIU will review the notification within 4 business days from receipt, and subject to its investigation, it will either initiate a freeze of assets and notify the Branch thereof or it will notify the Branch that the conditions for initiating a freeze of assets are not met.

IX.3. Freezing of assets

If the authority finds, either as a result of the information officially known to it or the investigation carried out on the basis of the notification, that the subject of the financial and proprietary restrictive measures has assets in Hungary that shall be frozen, it shall notify the reporting Branch immediately after the investigation by sending it the results of the investigation. It will also notify the Branch if the conditions for freezing are not met.

The transaction that may affect the assets which are subject to the financial and proprietary restrictive measures on the basis of the data, fact, and circumstances serving as basis for the notification, shall not be carried out

within 4 business days after the notification, unless the authority informs that the conditions for freezing are not met.
The transaction must be conducted on the 5th business day following the notification - provided that the other conditions for its execution are met - unless the authority sends a notification about ordering the freezing procedure.

The execution of the freezing procedure shall be ordered against the subject of financial and proprietary restrictive measure for those assets which are subject to financial and proprietary restrictive measures.

If, despite the prohibition on the provision of assets set out in the UNSC resolution, assets are made available to the subject of financial and proprietary restrictive measures, a decision shall be taken on their implementation and the authority shall be notified without delay.

The notification shall include the following information:

In case the subject of financial and proprietary restrictive measures is a natural person:

1. first and last name,
2. first and last birth name,
3. citizenship,
4. place and date of birth,
5. mother's maiden name,
6. address, if that is not available, place of residence,
7. type and number of identification document;

In case the subject of financial and proprietary restrictive measure is a legal person or unincorporated organisation:

- name, abbreviated name,
- address of its registered seat or, in the case of an entity based abroad, its branch in Hungary,
- names and positions of the authorised representatives,
- identification data of its delivery agent,
- in case of a legal person registered in the company register, the company registration number, in case of other legal persons, the number of the decision on its establishment (registration, recording) or its registration number;

furthermore:

- any other identifying information published by resolution of the UNSC imposing financial and proprietary restrictive measures;
- all data of the natural person, legal person, unincorporated organisation who has the right to restrict the implementation of the financial and proprietary restrictive measures on the assets subject to the financial and proprietary restrictive measures, as specified in the section determining the data of the natural person subject to the financial and proprietary restrictive measures.

as well as:

- the indication of the relevant provisions of applicable resolutions of the UNSC,
- all identification data of the legal person or unincorporated organisation who has the right to restrict the implementation of the financial and proprietary restrictive measures on the assets, as specified and available by law in accordance with the organizational form of the legal person or unincorporated organisation,

- the data necessary and available to identify the property.

PART 3: PROVISIONS COMMON TO THE IMPLEMENTATION OF THE AML / CFTR AND THE RESOLUTIONS OF UNSC

X. RIGHTS AND OBLIGATIONS OF THE DESIGNATED PERSON AND EMPLOYEES CONNECTED WITH THE CLIENT

X.1. The designated person

The Branch shall designate one or more persons (designated person) to perform the functions specified in the AML / CFTR and the resolutions of UNSC. The designated person must only be an employee of the Branch. Name and contact details of the designated person:

The designated person/ Money Laundering Reporting Officer (MLRO)/

name: Péter Marton
position: General Manager, MLRO
phone number: 06 30 400 7586
e-mail address: peter.marton@drnagye-qfcbranch.qa

The FIU shall be informed of the name, position, and contact details of the designated person from the date of commencement of his activities, as well as of any changes in these within five business days of the change. The Branch will send information to the FIU about the name and position of the designated person and any changes to them.

The designated person shall immediately forward the notification from the notifier to the FIU in the form of a protected electronic message, the receipt of which shall be immediately confirmed by the FIU via an electronic message.
The designated person is responsible for the quality of the reports, including in particular the accuracy, completeness, and due documentation of their data content.

Responsibilities of the designated person:

- availability to provide professional guidance to the employee,
- checking the content and form of the reports received by him and forwarding them to the FIU immediately,
- providing the FIU with details of the identity of the employee initiating the report, if expressly requested by the FIU,
- elaboration, operation, and development of the screening-monitoring system,
- in case of information indicating unusual transactions, request information from the employee related to the client and send this information in the form of a report,
- carrying out the FIU's request prepared and sent in accordance with the applicable legislation,
- organizing regular education and trainings for employees at least once a year including the sharing of up-to-date experience,
- elaborating the purpose, task, order, and rules of the activity related to the prevention and countering of money laundering and terrorist financing and the implementation of financial and proprietary restrictive measures.

The examples above is not exhaustive, and must extend, but does not limit, the meaning of these rules or particular provisions of these rules to which relates, for example as per Part 2.3.3 and 2.3.4 of the AML/CFTR regarding the general and particular responsibilities of the MLRO. In other matters relating to the MLRO such as Part 2.3.1, 2.3.2, 2.3.5 and 2.3.6 and Part 2.3.C regarding the MLRO reporting obligations.

Rights of the designated person:
- the designated person has the right to ask the reporting employee to supplement the received report.

X.2. Rights and obligations of the administrator having direct relation with the client

General behaviour towards the client:
Branch employees are obliged to get to know the management of all customers as well as possible. They shall strive to get to know the client as well as possible. If an employee detects an unusual transaction or they shall consult with the designated person and continue to act in an unobtrusive manner and shall refer to technical obstacles in the event of any disruption.

Responsibilities:

- classification of the client into a risk category,
- implementation of screening measures,
- continuous monitoring of the business relationship,
- filling in the notification form if any information, fact, or circumstance indicating money laundering or terrorist financing arises,
- filling in the notification form in case of funds or economic resources that are subject to the financial and proprietary restrictive measure (if he becomes aware of such),
- attaching to the report the documents supporting the detailed description of the information, fact, or circumstance indicating the financing of money laundering, terrorist financing or the existence of funds or economic resources subject to the financial and proprietary restrictive measures,
- immediate transmission of the completed report form to the designated person,
- keeping the report or the investigation as a secret from the client,
- participating in the related training program.

Rights:

- the right to request professional guidance from the designated person,
- the right to anonymity, according to which the name of the acting employee may not appear on the reports,
- exemption from the confidentiality obligation when initiating the submission of a report in good faith, whether or not it has been substantiated.

The designated person is responsible for the implementation of the obligations arising from the AML / CFTR by the employees.

Failure by the Branch employees or the designated person to comply with their due diligence or reporting obligations, whether intentionally or negligently, may result in employment, civil, and criminal repercussions. Liability may be established if an employee fails to comply with his or her due diligence obligations or fails to report an unusual transaction.

XI. DATA PROTECTION, REGISTER AS Part 7.1 AND 7.2 OF THE AML/CFTR

Records must be kept in a retrievable and verifiable manner about

- the personal and non-personal data, documents, and copies of documents recorded during client due diligence (including those generated during electronic identification),
- the report,
- the documents of the suspended transaction,
- actions taken at the request of the FIU, and
- official, prosecutorial, and judicial inquiries and the information provided pursuant to them.

All of the below items recorded in the process shall be kept for 10 years:

- in case of data, documents, or copies thereof, starting from the recording of data, whereas
- in case of the document proving the execution of the report and the suspension of the execution of the transaction order, as well as a copy thereof, and
- all other documents created in connection with the business relationship or copies thereof

shall be kept starting from the date of notification or suspension.

The document certifying the suspension of the transaction or a copy thereof, and the documents of the report shall be handled separately within the register.

The retention period applicable for the data, document, or a copy of the document obtained during the establishment of the business relationship begins upon the termination of the business relationship.

Personal data obtained in the course of fulfilling the client due diligence obligation shall be disclosed and processed only for the purposes of the tasks to be performed in order to prevent and counter money laundering and terrorist financing, to the extent necessary for the performance thereof.

The data, document and a copy of the document shall be kept in the register for the period specified in the request of

- the supervisory authority,
- the FIU,
- the investigating authority, the public prosecutor's office or the court,

but, in any case, not exceeding 10 years. The Branch will comply with the request without delay, but no later than the deadline specified in the request.

This is only possible if the data, document or copy of the document specified in the request is necessary for the conduct of an ongoing or future official procedure.

The above data, documents and their copies must be deleted or destroyed immediately after the expiry of the retention period.

The data, the document or a copy of the document shall be deleted immediately after the requesting authority, the public prosecutor's office or the court has been notified of the conclusion of the official proceedings and the failure to initiate the planned proceedings. The designated body shall immediately notify the Branch of the conclusion of the proceedings and the failure of the proceedings to be instituted.

In case of any information which changed due to a change or modification of the data, the old information must be preserved in such a way that the old data that are no longer in force and the dates of the data changes can be clearly established from it.

The Branch shall ensure the preservation of client data, declarations and documents, as well as copies thereof, on paper as part of the offer documentation or electronically in the Branch's electronic system.

The examples above is not exhaustive, and must extend, but does not limit, the meaning of these rules or particular provisions of these rules to which relates, as per Part 7.1 and 7.2 of the AML/CFTR.

XII. TRAINING PROGRAM

The Branch shall ensure that its employees involved in the conduct of activities under the AML/CFTR are familiar with the legal provisions for the prevention and countering of money laundering and terrorist financing, can identify the business relationship, transaction that enables or implements money laundering or terrorist financing, and that they are able to act in accordance with the AML/CFTR in the event of the occurrence of any data, facts or circumstances indicating money laundering or terrorist financing. It shall also ensure that its employees that are involved in the conduct of its activities under the AM /CFTR are familiar with the provisions of international and domestic laws concerning financial and proprietary restrictive measures imposed by the UNSC and that they comply with the obligations set forth therein.

To ensure this obligation, the designated person shall provide trainings to employees within 30 days from joining the company and shall provide them with further trainings at least once a year thereon.

Should the employee be prevented from attending the training, they must make sure to attend within 30 days from the end of the impedance.

The knowledge acquired during the trainings shall be tested by a written exam. If the employee is prevented from taking the exam, they re-sit within 30 days from the end of the impedance.

The Branch will retain the training and exam materials, the answer keys, the list of candidates and the exam results of each candidate for 10 years starting from the date of the exam.

The training program (as per Part 6.2.1 (2) of the AML/CFTR regarding the minimum training program) includes the following topics:

the statutory definitions and legal analyses of the following crimes punishable as a criminal offence under the laws of Qatar:

- act of terrorism,
- violation of an international economic ban,
- breach of economic secrecy,
- money laundering,
- failure to comply with the obligation to report money laundering, AML/CFTR and

a description of the concepts set out in the law on the implementation of the financial and proprietary restrictive measures ordered by the UNSC,
mandatory cases of client due diligence,
client due diligence measures in case of:

- client due diligence based on AML/CFTR,
- simplified client due diligence,
- enhanced client due diligence, and
- client due diligence performed by another service provider,

records used during client due diligence,
detailed rules for fulfilling the reporting and suspension obligation,
the prohibition disclosure and its practical significance,
activities related to the prevention and combating of money laundering and terrorist financing; and

- data protection,
- recording, and
- statistical

issues arising in relation to the implementation of the financial and property restrictive measures ordered by the UNSC,

- the operational rules of the screening systems applied by the Branch in connection with the prevention and countering of money laundering and terrorist financing and the implementation of financial and proprietary restrictive measures ordered by the UNSC,
- a description of the concept of the enhanced procedure as well as the procedures and measures applied by the Branch under such enhanced procedure,
- the Branch specific aspects of the national risk assessment,
- the Branch's own policies, and
- the internal risk assessment of the Branch.

The Branch conducts client due diligence by means of audited electronic communication devices, therefore it does organize trainings on the relevant know-how either.

The Branch conducts training for higher-impact individual, (examples: a senior manager of the firm, the firm's MLRO or Deputy MLRO and, an individual whose role in the firm includes conducting any other activity with or for a customer; as per Part 6.1.1 of the AML/CFTR) in relation to a firm, means an individual who has a role in preventing money laundering or terrorism financing under the firm's AML/CFT programme.
A firm's screening procedures for the appointment or employment of officers and employees must ensure that an individual is not appointed or employed unless:
(a) for a higher-impact individual—the firm is satisfied that the individual has the appropriate character, knowledge, skills and abilities to act honestly, reasonably and independently; or
(b) for any other individual—the firm is satisfied about the individual's integrity.
The procedures must, as a minimum, provide that, before appointing or employing a higher-impact individual, the firm must:

(a) obtain references about the individual;
(b) obtain information about the individual's employment history and qualifications;
(c) obtain details of any regulatory action taken in relation to the individual;
(d) obtain details of any criminal convictions of the individual; and
(e) take reasonable measures to confirm the accuracy and completeness of information that it has obtained about the individual.

The designated person is responsible for the development and implementation of the training program and for the training of the employees and for higher-impact individual.

XIII. CLOSING PROVISIONS

The above rules shall apply to contractual relations with a new client or to new transaction orders established after the entry into force of this policy.

Doha, 01/09/2020
Dr Nagy Business Consulting QFC Branch

Schedule 1 – Identification form
ONLY THE SERVICE PROVIDER MAY FILL IT IN! – applicable upon the establishment of the business relationship

Data of natural person (Please put an X where applicable):

First and last name:										
First and last name upon birth:										
Citizenship:	Hungarian:		Other:							
Place and date of birth:					year		month			day
Mother's maiden name:										
Address, or, if not applicable, place of residence:										
Type of identification card:	Identity card		Address card		Driving license		Passport		Official document suitable for identification purposes	Other
Name of other identification document:										
Numbers in order:										

Data of legal person or an unincorporated organisation (applicable for private entrepreneurs too):

Name, abbreviated name:	
Registered seat, address of Hungarian branch:	
Main scope of business:	
Name and title of authorized representative:	
Data of agent for service of process:	
Company registration/decision, reference number:	

Tax number:																					

Data recorded by:

_____ _____

name date

I hereby declare under perjury of prejudice that the above data are valid and the same as those contained in my personal documents presented to the person carrying out the identification process. I am aware that any eventual change in the above data or in my personal data shall be reported to Dr Nagy Business Consulting QFC Branch within five business days, and I am responsible for any damages caused by the failure to do so.

Dated: _____,_____/_____/_____ Client's signature: _____

Schedule 2 – Customer's beneficial ownership statement
TO BE COMPLETED BY A NAUTRAL PERSON! - Declaration by the authorized person in case of a contractual relationship

In case of business relationship:
I, the undersigned …… declare that I am acting as a natural person on behalf of the following person(s):*

In case of a transaction order:
I, the undersigned ……, (as the representative of ……) declare that I am acting on behalf of the following person(s) as a proxy, holder, and representative:

1.		1.	
2.		2.	
3.		3.	
4.	5. 6.	4.	5. 6.
7.		7.	
8.	yes: no:	8.	yes: no:
9.	10. %	9.	10. %
1.		1.	
2.		2.	
3.		3.	
4.	5. 6.	4.	5. 6.
7.		7.	
8.	yes: no:	8.	yes: no:
9.	10. %	9.	10. %

1: First and last name:
2: First and last birth name:
3: Address or, if not available, place of residence:
4: Citizenship:
5: Hungarian– mark with an X, do not fill in field 6.
6: Other (in case of a client who is a non-Hungarian citizen, enter the citizenship):
7: Date and place of birth:
8. Whether the beneficial owner qualifies as a politically exposed person - mark with an X. (If yes, please fill in the statement of the politically exposed person beneficial owner)

9: Nature of ownership interest **
10. Degree of ownership interest **

I am aware that within 5 (five) working days I am obliged to notify the service provider of any changes in the above data or in my own data and the damage resulting from the failure to comply with this obligation shall be borne by me.

Place: ……., ……. day ……. month ……..……

……
Signature of the client

* The appropriate part should be underlined or highlighted.
** Please fill in only if you are acting on behalf of a legal entity in case of an authorized transaction order.

Beneficial owner
[Only the categories corresponding to the activity of the Service Provider should be listed]

Schedule 3 – Customer's beneficial ownership statement

TO BE COMPLETED BY A LEGAL ENTITY OR AN ORGANIZATION WITH NO LEGAL ENTITY!

- If the client is a legal entity, a statement by the representative in case of a contractual relationship!

I, the undersigned ……, (as the representative of ……..…….) declare that the beneficial owner(s) of the legal person or unincorporated organisation I represent is (are) the following person(s):

1.		1.	
2.		2.	
3.		3.	
4.	5. 6.	4.	5. 6.
7.		7.	
8.	9. %	8.	9. %
10.		10.	
1.		1.	
2.		2.	
3.		3.	
4.	5. 6.	4.	5. 6.
7.		7.	
8.	9. %	8.	9. %
10.		10.	

1: First and last name:
2: First and last birth name:
3: Address or, if not available, place of residence:
4: Citizenship:
5: Hungarian– mark with an X, do not fill in field 6.
6: Other (in case of a client who is a non-Hungarian citizen, enter the citizenship):
7: Date and place of birth:
8. Whether the beneficial owner qualifies as a politically exposed person - mark with an X. (If yes, please fill in the statement of the politically exposed person beneficial owner)
9: Nature of ownership interest **

10. Degree of ownership interest **

I am aware that within 5 (five) working days I am obliged to notify the service provider of any changes in the above data or in my own data and the damage resulting from the failure to comply with this obligation shall be borne by me.

Place: ……., ……. day ……. month ……. year

……

Signature of the client

Beneficial owner:
[Only the categories corresponding to the activity of the Service Provider should be listed]

Schedule 4 Beneficial Owner's politically exposed person's statement
TO BE COMPLETED BY A CUSTOMER! *- Additional statement in Schedule 3 as to whether the beneficial owner is a key public figure!

I, the undersigned ……., (as the representative of …….) declare that the beneficial owner of the legal person or unincorporated organisation I represent is …….

Politically exposed person (enter the category code according to point A.)	A/
Family members of a politically exposed person (enter the category code according to point B.)	B/
Close associates of a politically exposed person (enter the category code according to point C.)	C/

A

a)	heads of State, heads of government, ministers and deputy ministers, state secretaries
b)	members of parliament or of similar legislative bodies
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
e)	members of courts of auditors or of the boards of central banks,
f)	ambassadors, chargés d'affaires and high-ranking officers in the armed forces
g)	g) members of the administrative, management or supervisory bodies of enterprises with majority state ownership
h)	directors, deputy directors and members of the board of an international organization

B

a)	Spouse
b)	Domestic partner
c)	Biological and adopted children, stepchildren and foster children
d)	Spouses or domestic partners of the above
e)	Biological, adoptive, step- and foster parents

C

a)	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)	the sole beneficial owner of a legal entity or unincorporated organization which is known to have been set up for the benefit of a politically exposed person

Source of funds	

Place and date:……., ……..year……..month……..day

…….
signature

Schedule 5 – Politically exposed person's statement
TO BE COMPLETED BY A NATURAL PERSON!

I declare that I am not a politically exposed person (mark with an X)	
I declare that I am a politically exposed person (enter the category code according to point A)	A/
I declare that I am a family member of a politically exposed person (enter the category code according to point B)	B/
I declare that I am a close associate of a politically exposed person (enter the category code according to point C)	C/

A

a)	heads of State, heads of government, ministers and deputy ministers, state secretaries
b)	members of parliament or of similar legislative bodies
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
e)	members of courts of auditors or of the boards of central banks,
f)	ambassadors, chargés d'affaires and high-ranking officers in the armed forces
g)	g) members of the administrative, management or supervisory bodies of enterprises with majority state ownership
h)	directors, deputy directors and members of the board of an international organization

B

a)	Spouse
b)	Domestic partner
c)	Biological and adopted children, stepchildren and foster children
d)	Spouses or domestic partners of the above
e)	Biological, adoptive, step- and foster parents

C

a)	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)	the sole beneficial owner of a legal entity or unincorporated organization which is known to have been set up for the benefit of a politically exposed person

Source of funds	

Place and date:……..., ……..year……..month……..day

…….…….
signature

Schedule 6 – Reporting of information, fact or circumstance indicating the occurrence of money laundering and terrorist financing
FOR INTERNAL USE ONLY!

The report shall be accompanied by available documents indicating the existence of data, facts, and circumstances implying money laundering and terrorist financing.

1. Dr Nagy Consulting QFC Branch (head office: …; telephone number: ……)

   1.1. Name and address of the (unit) detecting the suspicious transaction (if not the same as in point 1)
   1.2. Date and time of detection
   1.3. Registration numbers and dates of previous notifications concerning the same case (client) (if any):
   1.4. Name, work address, telephone number of the designated person

2. Identification of the involved client (relevant data according to AML / CFTR)
   2.1. All credentials are available: Yes / No
   2.2. Is there another person involved in the case? If yes, details of related and other person(s) [indicate also the person to whom the transaction is conducted (if any)]

3. Details of the transaction (including the transaction conducted or to be conducted and the transaction initiated but not conducted by the client)
   3.1. Description of the transaction (type, total amount by currency, payment, transfer, receipt of amount, credit transfer, etc.)
   3.2. Type(s) and number(s) of clients and beneficiary accounts, if any
   3.3. A description of data, fact, or circumstance implying money laundering or terrorist financing
   < **Describe here why the client has become suspicious, why the transaction is unusual, why the report is being made** >
   3.4. Documents supporting the description of data, fact, or circumstance implying money laundering or terrorist financing, if available [copy of the customer's contracts with the Service Provider, reference documents, other detailed descriptions, remarks, notes, etc.]

4. Other data, facts or circumstances, not described above, which indicate money laundering or terrorist financing

5. Measures taken by the service organization.

Place:……., ……..day……..month…….year

Schedule 7 – Contact details of the FIU

Address: Qatar's National Financial Crime Centre, Building 11, 8th Floor Al Baladiya Street 810, Doha - Qatar
P.O. Box 1234
Telephone No.: +974 4422 1511
Fax No.: +974 4422 1773
Email: info@qfiu.gov.qa
Website: http://www.qfiu.gov.qa

Reporting Entities must submit STRs through the QFIU Electronic STR System (E-STR).

Schedule 8 - Contact details of the lists relevant to the prevention and countering of money laundering and terrorist financing and compliance with embargo restrictions

United Nations Security Council
https://www.un.org/sc/suborg/en/

United Nations Sanctions
https://www.un.org/sc/suborg/en/sanctions/information

Wolfsberg Group Country Risk Frequently Asked Questions (FAQs) 2018
https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20FC%20Country%20Risk%20FAQs%20Mar18.pdf

Basel AML Index 2019 Report
https://www.baselgovernance.org/sites/default/files/2019-08/Basel%20AML%20Index%202019.pdf

Financial Action Task Force High-risk and non-cooperative jurisdictions
http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

Financial Action Task Force Improving Global AML/CFT Compliance: On-going Process 18 October 2019
http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/public-statement-october-2019.html
http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2017.html

Financial Markets Authority – New Zealand
Countries Assessment Guideline
https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/guidance-and-publications/4853287.pdf?la=en

Organisation for Economic Co-operation and Development
List of Unco-operative Tax Havens
http://www.oecd.org/countries/monaco/listofunco-operativetaxhavens.htm

The Financial Secrecy Index
https://www.financialsecrecyindex.com/introduction/fsi-2018-results

Transparency International Corruption Perception Index 2018
https://www.transparency.org/files/content/pages/2018_CPI_Executive_Summary.pdf

European Union Sanctions
https://www.sanctionsmap.eu/#/main?search=%7B%22value%22:%22%22,%22searchType%22:%7B%22id%22:1,%22title%22:%22regimes,%20persons,%20entities%22%7D%7D

World Bank World Governance Indicators

http://info.worldbank.org/governance/wgi/#home

Fragile States Index
http://fundforpeace.org/fsi

Global Terrorism Database
https://www.start.umd.edu/gtd/
The Government of UK – guidance on sanctions, embargoes and restrictions
March 2016
https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions

Schedule 9 – Reporting based on financial and proprietary restrictive measures
FOR INTERNAL USE ONLY!

Guidance to Submitting Suspicious Transaction Reports, SCHEDULE-B, **QFIU Suspicious Transaction Report Form**

Schedule 10 - Typical behaviours of money laundering and terrorist financing

1. Money laundering:
   - sudden, significant increase in extraordinary / ad hoc payments / payments for either an individual or a legal entity;
   - a significant amount of money does not fit the client's profile;
   - regular transactions directly below the identification threshold;
   - payments and withdrawals that do not fit the client's profile;
   - use of the service differently than the usual conduct;
   - a company that is reluctant to provide complete information about its business purpose, previous banking relationships, officers, directors, or place of business;
   - a client who refuses to provide information when entering into a contract;
   - a client who wishes to conclude a contract without references, local address, or personal identification (e.g. passport, driver's license), or who refuses to provide any other information required by the insurer for the conclusion of the contract;
   - a client who provides information that appears to be very minimal or possibly false, or cannot easily verify, especially regarding their identity;
   - an unjustified, significant difference from traditional business methods;
   - the client attempts to enter into a transaction, enters into a contract above a certain threshold, but when informed of the registration or reporting requirements, withdraws from the contract in order to keep the transaction just below that threshold;
   - the client wishes to deposit money and insists on not filling in the required registration or reporting forms not be filled out;
   - the client enters into many contracts below the identification threshold;
   - a customer who is reluctant to provide identifying information or to continue the transaction after being informed that they must identify themselves;
   - a client who forces or attempts to force an employee to not submit the required registration or reporting forms.

2. Transactions giving rise to suspicion of terrorist financing:

Terrorists typically make sure that they do not cause any inconvenience or suspicion with their behaviour in their environment, relationship system or financial habits. Therefore, the description of unusual transactions is not or difficult to type in relation to them.

Terrorists also collect illegal and typically seemingly legal resources: in addition to defence money, blackmail and drug and arms trafficking, they also raise funds from foundations and non-profit organizations that operate legally and collect membership fees and sell publications.

For instance, it may cause suspicion when several people terminate their funds held on trust and ask to pay the same amount of money to the same person.

Schedule 11 - Risk-based analysis