

**Date:** 2/7/2019

**Number:** MJ/D/2/7/2

**Ministerial Decision No. (533) of 2019**

**On Anti-Money Laundering and Combating Terrorism Financing related to Lawyers, Notaries and Legal Independent Professionals**

The Minister of Justice

And After having perused the Constitution;

Federal law No (1) of 1972 on competencies of ministries and capacities of ministers, as amended;

Federal law No (23) of 1991 regulating legal practice, as amended, and its implementing regulations;

Federal law No (11) of 1992 on civil procedures, as amended, and its implementing regulations;

Federal law No (8) of 2004 on financial free zones and its implementing regulations;

Federal law No (13) of 2007 on commodities subject to control of import and export, as amended;

Federal law No (4) of 2013 regulating notary public work, as amended, and its implementing regulations;

Decree by federal law No (20) of 2018 on anti-money laundering, Combating Terrorism finance and finance of illegal organizations;

Cabinet resolution No (23) of 2008 on the organizational structure of the Ministry of Justice, as amended;

Cabinet resolution No (10) of 2019 on the implementing regulations of decree by federal law No (20) of 2018 on anti-money laundering, Combating Terrorism finance and finance of illegal organizations;

Cabinet resolution No (20) of 2019 on the system of lists of terrorism and application of Security Council resolutions relating to ban and suppression of terrorism and its finance, and combatting armament proliferation and its finance, and related resolutions;

Cabinet resolution No (3/1f) of 2019 issued on 08/01/2019 approving the Ministry of Justice as supervisory authority of lawyers and notaries public in the State; and

Ministerial decree No (532) of 2019 establishing Department of Anti-Money Laundering and Combating Terrorism Finance Department,

Decided:

## **Article (1)**

### **Definitions**

In Implementation of the provisions of this decision, the following terms and expressions shall have the meaning assigned next to each; unless otherwise the context so requires:

<b>The State</b>	:	The United Arab Emirates
<b>The Ministry</b>	:	The Ministry of Justice
<b>The Minister</b>	:	The Minister of Justice
<b>The Undersecretary</b>	:	The Undersecretary of the Ministry of Justice
<b>The Committee</b>	:	The National Committee for Anti-Money Laundering and Combating Terrorism Financing and the Financing of Illegal Organizations
<b>The Unit</b>	:	The Financial Intelligence Unit
<b>The Office</b>	:	The Executive Office for Goods and Material Subjected to Import and Export Control
<b>The Section</b>	:	The Anti-Money Laundering and Combating Terrorism Financing Section established in the Ministry in accordance with the Ministerial Decision No. (532) of 2019
<b>Designated Non-Financial and Businesses Professions (DNFBPs)</b>	:	Lawyers, Notaries and other legal independent professionals, as the case may be
<b>The Supervised Sector</b>	:	The DNFBPs sector subject to the supervision of the Ministry as per this Decision
<b>The Relevant Authorities</b>	:	The Governmental authorities concerned with the implementation of any of the provisions of the Decretal Law in the State
<b>The Predicate Offense</b>	:	Any act constituting an offense or misdemeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.

- Money Laundering** : Any of the acts specified in Clause (1) of Article (2) in the Decretal Law
- The Crime** : Money laundering crime and related Predicate Offences, or Financing of Terrorism or Illegal Organizations.
- Funds** : Assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any form including electronic or digital forms or any interests, profits or income originating or earned from these assets.
- Freezing** : Temporary restriction over the moving, conversion, transfer, replacement or disposition of funds in any form, by an order issued by a Competent Authority.
- Suspicious Transactions** : Transactions related to funds for which there are reasonable grounds to suspect that they are earned from any felony or misdemeanor related to the financing of terrorism or of illegal organizations, whether committed or attempted.
- Suspicious Transaction Report** : A report in which the DNFBPs shall raise to the Unit upon suspicion of a transaction
- Legal Arrangement** : A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality such as trusts or other similar arrangements.
- Trust** : A legal relationship in which a settlor places funds under the control of a trustee for the interest of a beneficiary or for a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor.
- Settlor** : A natural or legal person who transfers the control of his funds to a Trustee under a document.
- Trustee** : A natural or legal person who has the rights and powers conferred to him by the Settlor or the Trust, under which he administers, uses, and acts with the funds of the Settlor in accordance with the conditions imposed on him by either the Settlor or the Trust.
- Shell Bank** : Bank that has no physical presence in the country in

- which it is incorporated and licensed, and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
- Customer** : Anyone who performs or attempts to perform any of the acts defined in Articles (2) and (3) of the present Decision with any Financial Institution or Designated Non-Financial Business or Profession.
- Beneficial Owner** : The natural person who owns or exercises effective ultimate control, directly or indirectly, over a Customer or the natural person on whose behalf a Transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal Arrangement.
- Transaction** : All disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation.
- Business Relationship** : Any ongoing commercial or financial relationship established between financial institutions, designated non-financial businesses and professions, and their Customers in relation to activities or services provided by them.
- Due Diligence** : Process of identifying or verifying the information of a Customer or Beneficial Owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it for the purposes of the Decretal-Law and this Decision.
- Enhanced Due Diligence (EDD)** : The measures identified in Article (21) of this Decision
- High Risk Countries** : The countries included in the high risk category on the international level, as per the list issued from FATF or as identified by the Committee
- High Risk Customer** : A Customer who represents a risk either in person, activity, business relationship, nature of geographical area, such as a Customer from a high-risk country or non-resident in a country in which he does not hold an identity card, or a customer having a complex structure, performing complex transactions or having unclear economic or legal objective, or who performs cash-intensive transactions, or transactions with an unknown third

- party, or non-face-to-face transactions or any other high risk transactions identified by the Section or the DNFBPs
- Local List** : The list issued by the Cabinet to list persons or organizations in the local terrorists list in accordance with the provisions of Article (3) of Cabinet Resolution No. (20) of 2019 concerning regulating terrorists lists and implementing UN Security Council resolutions on prevention and suppression of terrorism and terrorism financing and combating proliferation of and its financing.
- Sanctions List** : A list of which contains the names of terrorist individuals or organizations subject to sanctions prescribed in accordance with the Sanctions Committee affiliated to the Security Council and the related information to such individuals or organizations and the grounds of listing therein
- The Designated** : A person or entity listed by the UNSCRs in the Sanctions List or listed in accordance with the Cabinet Resolution in the Local List, as the case may be
- :  
**Decretal Law** : Federal Decretal Law No. (20) of 2018 on Anti-Money Laundering and Combating Terrorism Financing and the financing of Illegal Organizations
- The Executive Regulation (By-Law)** : Cabinet Decision No. (10) of 2019 concerning the Executive By-Law of Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations

## **Chapter One**

### **Objectives and Scope of Enforceability**

#### **Article (2)**

##### **Objectives of the Decision**

This Decision aims to establish procedures and controls for monitoring, supervision and follow-up DNFBPs subject to the supervision of the Ministry to ensure their compliance with the provisions of Decretal Law and its By-Law, and this Decision.

#### **Article (3)**

##### **Scope of Enforceability**

- 1- The provisions of this Decision shall apply to DNFBPs in the State, including free zones and financial free zones.  
The Ministry may seek assistance from the authorities managing the free zones and financial free zones to follow-up the implementation of the provisions of Decretal Law and its By-Law, and this Decision in those free zones.
- 2- DNFBPs shall apply this Decision upon preparing and carrying out Financial Transactions or upon executing to the interest of their Customers with regards to the following activities:
  - 1) Purchase and sale of real estate.
  - 2) Management of Funds owned by the Customer.
  - 3) Management of bank accounts, saving accounts or securities accounts.
  - 4) Organizing contributions for the establishment, operation or management of companies.
  - 5) Creating, operating or managing Legal Persons or Legal Arrangements.
  - 6) Selling and buying commercial entities.
- 3- The provisions of this Decision shall be inapplicable when DNFBPs conduct assessments to the legal status of their Customer, defend or represent him/her before the law, arbitration or intermediation, or upon giving legal opinion in matters related to legal procedures, including consultancy on initiating or avoiding conducting such procedures or under any other circumstances they become subject to professional privilege other than those cases set out in the Decretal Law and its By-law.

## **Chapter Two**

### **Supervision on DNFBPs**

#### **Article (4)**

#### **Anti-Money Laundering Section**

The Anti-Money Laundering Section, established under the Ministerial Decision No. (532) of 2019 aforementioned; shall monitor, follow-up and supervise DNFBPs, in accordance with the Competences specified in Article (5) of this Decision

#### **Article (5)**

#### **Competences of the Section:**

The Section, in doing its functions, shall have the following competences:

1. Conduct risk assessment to the potential commitment of crime in the sector under supervision.
2. Establish a hard or soft database for DNFBPs that include all data related to them, namely; name, type, activity, commencement date, and copy of the license. And to keep it updated on on-going basis
3. Find effective and rapid means to online communication with DNFBPs, independently or collectively
4. Receive inquiries and provide assistance and support to DNFBPs, by email of the Section, hotline dedicated to this purpose or any other means.
5. Train personnel of the Section on periodic basis
6. Follow-up and implement the operational plan for Anti-Money Laundering and Combating Terrorism Financing by the Ministry.
7. Carry out offsite and onsite supervision and inspection on DNFBPs based on the following:
  - A. National Risk Assessment issued by the Committee.
  - B. Risks of crime and internal policies and controls and procedures related to the sector under supervision as specified in the Risk Assessment prepared to the best knowledge of the Section.
8. Keep updated list of the names and data of compliance officers in DNFBPs and advise the Unit therewith.

9. Prepare Risk Assessment Questionnaire Form, Suspicious Transaction Report Form and any other related forms, in coordination with the Unit, and provide DNFBPs with.
10. Organize programs and awareness campaigns to DNFBPs and their staff on combating crime and to provide them with guidelines and feedback to enhance effective implementation of combating crime measures.
11. Verify the compliance of DNFBPs with implementation of the obligations set forth in Decretal Law, Executive Regulation and this Decision, particularly the implementation of Enhanced Due Diligence measures and on-going supervision of Business Relation on Customers related to High Risk Countries.
12. Take all measures to ensure compliance of DNFBPs with the implementation of UNSCRs related to the prevention and suppression of terrorism and terrorism financing and combating proliferation of weapons of mass destruction and its financing, and other relevant resolutions, by onsite visits and on-going follow-up, and to pose proportionate administrative sanctions upon violation or default in implementing the instructions.
13. Report back to the Office of the notices and data received from DNFBPs regarding the Designated.
14. Prepare reports on violations from DNFBPs and refer them to the Undersecretary.
15. Advise DNFBPs with the decisions made with respect to the administrative sanctions imposed on them.
16. Advise the Unit with the reasoning behind the sanction decision and the grievance therefrom.
17. Prepare regular statistics on the measures taken and sanctions imposed, and key performance indicators.
18. Any other competences of Supervisory Authorities contained in the decretal law and its Executive Regulation, and the aforementioned Cabinet Resolution No. (20) of 2019.



## **Chapter Three**

### **Obligations of BNFBBs**

#### **Article (6)**

DNFBPs shall implement all provisions and obligations set forth in Decretal Law and its Executive Regulation, and the aforementioned Cabinet Resolution No. (20) of 2019, particularly, the provisions and obligations set forth in this Chapter.

#### **Section One**

#### **Due Diligence Measures**

#### **Article (7)**

#### **Business Relationship Due Diligence Measures**

DNFBPs shall take Customers due diligence measures before establishing or progressing any Business Relationship, or executing a transaction.

DNFBPs shall not - in case failed to take such measures - establish, progress any Business Relationship, or execute a transaction, and They shall advise the Unit with Suspicious Transaction Report.

#### **Article (8)**

#### **Cases of taking Due Diligence Measures**

Customers Due diligence measures shall be taken in the following cases:

1. Establishing the business relationship;
2. Carrying out transactions in favor of a Customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
3. Carrying out occasional transactions in the form of Wire Transfers for amounts equal to or exceeding AED 3,500.
4. Where there is a suspicion of the Crime.
5. Where there are doubts about the veracity or adequacy of previously obtained Customer's identification data.

## **Article (9)**

### **Prohibitions**

DNFBPs shall be prohibited from performing the following dealings:

- A. Dealing in any way with Shell Banks, whether by opening bank accounts in their names, or accepting funds or deposits from them.
- B. Creating or keeping records of bank accounts using pseudonyms, fictitious names or numbered accounts without the account holder's name.

## **Section Two**

### **Customer Identification**

#### **Article (10)**

Identification of the Customer before the Business Relationship

DNFBPs, before or during the establishment of the Business Relationship or opening an account, or before executing a transaction for a Customer with whom there is no Business Relationship, verify the following:

1. Identity of the Customer and Beneficial Owner; whether permanent or occasional, natural or legal person or arrangement, by using documents or data from a reliable and independent source, or other information to identify the identity as stipulated in article (12, 13 and 14) of this Decision.
2. Any person act on behalf of the Customer, and to verify the identity of that person as outlined in Clause (1) of this Article.
3. Understand the purpose of the Business Relationship and its nature and obtain information related to the purpose thereof when necessary.
4. Understand the nature of the Customer's Business Relationship, structure of ownership and control over the Customer.

Except for what is contained in paragraph 1 above, in the cases where there is a low crime risk, and after having completed the risk management measures approved by the senior management, it is permitted to complete verification of Customer identity after establishment of the business relationship, under the following conditions:

- A. The verification will be conducted in a timely manner as of the commencement of Business Relationship or the implementation of the Transaction..
- B. The delay is necessary in order not to obstruct the natural course of business.
- C. The implementation of appropriate and effective measures to control the risks of the Crime.

### **Article (11)**

#### **Verifying the identity for Natural Person Customer**

Verification of identity for Customers and Beneficial Owners of natural persons shall be as follow:

- 1. Name as in the ID card or passport, along with attaching valid copy of the original from the ID card and passport
- 2. Nationality
- 3. Address and Place of Birth
- 4. Name and Address of Employer
- 5. Obtaining senior management's approval if the Customer or the Beneficial Owner is a PEP.

### **Article (12)**

#### **Verifying the identity for Legal Person Customer**

Verification of identity for customers and beneficial owners of legal persons shall be as follow:

- 1. The name, Legal Form and Memorandum of Association
- 2. Headquarter office address or the principal place of business; if the legal person or arrangement is a foreigner, it must mention the name and address of its legal representative in the State and submit the necessary documents as a proof.
- 3. Articles of Association or any similar documents, attested by the competent authority within the State.
- 4. Names of relevant persons holding senior management positions in the legal person or legal arrangement.

## **Article (13)**

### **Verifying the identity of Beneficial Owner**

DNFBs should take reasonable measures to verify and identify the identity of Beneficial Owners of legal persons and arrangements by using information, data, and documents obtained from reliable source, as follow:

1- For Customers that are legal persons:

- A. Obtaining and verifying the identity of the natural person, who by himself or jointly with another person, has a controlling ownership interest in the legal person of 25% or more, and in case of failing or having doubt about the information acquired, the identity shall be verified by any other means.
- B. In the event of failing to verify the identity of the natural person exercising control as per paragraph )A (of this Clause ,or the person)s ( with the controlling ownership interest is not the Beneficial Owner, the identity shall be verified for the relevant natural person(s) holding the position of senior management officer, whether one or more persons. .

2- For Customers that are Legal Arrangements:

Verifying the identity of the Settlor, the Trustee(s), or anyone holding a similar position, the identity of the beneficiaries or class of beneficiaries, the identity of any other natural person exercising ultimate effective control over the legal arrangement, and obtaining sufficient information regarding the Beneficial Owner to enable the verification of its identity at the time of payment, or at the time it intends to exercise its legally acquired rights.

## **Article (14)**

### **Cases of Exemption from verifying the Identity**

DNFBPs shall be exempted from identifying and verifying the identity of any shareholder, partner, or the Beneficial Owner, in the event where the Customer or the owner holding the controlling interest are as follow:

- 1. A company listed on a regulated stock exchange subject to disclosure requirements through any means that require adequate transparency requirements for the Beneficial Owner.
- 2. A subsidiary whose majority shares or stocks are held by the shareholders of a holding company.

And in all cases, evidencing information and documents shall be obtained from a reliable source.

### **Article (15)**

#### **On-going Supervision during Business Relationship**

DNFBPs should undertake CDD measures and ongoing supervision of Business Relationships, including:

1. Audit Transactions that are carried out throughout the period of the Business Relationship, to ensure that the Transactions conducted are consistent with the information they have about Customer, their type of activity and the risks they pose, including - where necessary - the source of Funds
2. Ensure that the documents, data or information obtained under CDD Measures are up-to-date and appropriate by reviewing the records, particularly those of High-Risk Customer categories

### **Article (16)**

#### **Suspicion in a crime**

DNFBPs may, upon suspicion of a crime, not implement the CDD measures unless they had reasonable grounds indicating that the implementation of such measures might tipp-off the Customer

And in that case, they have to advice the Unit through STR and mention the reasons that made them not implement such measures

### **Article (17)**

#### **Reliance on Third Party**

DNFBPs may rely on Third parties upon implementing the CDD measures, in accordance with the controls specified in Article (19) of the By-Law

## **Section Three**

### **Identify and Mitigate the Crime Risks**

#### **Article (18)**

##### **Identifying Crime Risks**

DNFBPs should identify the risks of Crime within the scope of their business and assess them in line with the nature and size of business, and they shall oblige to the following:

- 1- Fulfil and analyze the data of Template (1) attached herewith, in accordance with the results of the National Risk Assessment issued by the Committee.
- 2- Take into consideration all related factors of risk such as risks of Customers, Countries or Geographic areas, products, services, Transactions and its channels of delivery, before identifying the overall level of risks and the appropriate level of applicable procedures to mitigate the risks.
- 3- Documentation, updating risk assessment transactions on on-going basis and make them available upon request.

#### **Article (19)**

##### **Risk Mitigation**

DNFBPs shall mitigate the risks previously identified in accordance with the above-mentioned article or in accordance with the results of the National Risk Assessment, throughout the following:

- A. Developing internal policies, controls and procedures that are commensurate with the nature and size of their business and are approved by senior management, to enable them to manage the risks that have been identified, and if necessary, to monitor the implementation of such policies, controls and procedures and enhance them.
- B. Applying Enhanced CDD measures once high risks are identified.

## **Section Four**

### **Cases of taking Special Due Diligence Measures**

#### **Article (20)**

##### **Simplified CDD Measures**

In case the requirements stipulated in Articles (17 and 18) above are met, Professionals shall be permitted to apply simplified CDD measures to manage and limit the identified low risks, unless there is suspicion of a committed Crime. The simplified CDD measures should commensurate with the low risk elements. These include the following, as examples:

- A. Verify the identity of the Customer and Beneficial Owner after establishing the Business Relationship.
- B. Update the Customer's data based on less frequent intervals.
- C. Reduce the rate of ongoing monitoring and transaction checks.
- D. Deduce the purpose and nature of the Business Relationship based on the type of Transactions or the Business Relationship that has been established, without the need to gather information or performing specific procedure.

#### **Article (21)**

##### **Enhanced CDD Measures**

DNFBPs shall manage High Risks by taking enhanced CDD Measures such as:

- 1. Obtaining more information and investigating this information such as information relating to the Customer and Beneficial Owner identity, or information relating to the purpose of the business relationship or reasons of the transaction.
- 2. Updating the CDD information of the Customer and Beneficial Owner more systematically.
- 3. Taking reasonable measures to identify the source of the Funds of the Customer and Beneficial Owner.
- 4. Increasing the degree and level of ongoing Business Relationship monitoring and examination of Transactions in order to identify whether they appear unusual or suspicious.
- 5. Obtaining the approval of senior management to commence the Business Relationship with the Customer.

## **Article (22)**

### **Measures against High-Risk Countries and Customers**

1. DNFBPs shall implement the measures identified by the Committee with regards to High-Risk Countries
2. DNFBPs shall implement the Enhanced CDD Measures that commensurate with the level of risk that might arise from Business Relationship or Transactions with High-Risk Customers.

## **Article (23)**

### **Measures against Politically Exposed Persons (PEPs)**

DNFBPs shall implement CDD measures before or during the Business Relationship with PEPs in accordance with the By-Law

## **Article (24)**

### **Measures against the Designated**

DNFBPs, and for the purpose of verifying a Designated Customer, shall take the following measures:

1. Check the Sanctions List and the Local List through the Security Council's or the Office's, or the Ministry's website, before conducting a transaction or entering any serious Relationship with any person
2. Check, on on-going basis, the Customers' databases and any information obtained concerning potential Customers or current ones; and comparing the information with the listed names in the Sanctions List and the Local List; also, maintain an updated list, kept in the database for the listed terrorist persons and organizations list.
3. Take freezing measures immediately after having a match, or receiving an email from the Office. The freezing shall occur to the Funds in their possession, under their control or management, owned, controlled over or possessed, entirely or partially, directly or indirectly by the Designated, or any person acting on the Designated behalf, or under its directions, or be it owned, controlled over by it, directly or indirectly  
DNFBPs shall be prohibited from making available the Funds, of the Designated, held in their possession, under their control or management, or financial services, or others, whether directly or indirectly, for its behalf, unless by permission from the Office



4. Immediate notification to the Section, in case the freezing measures were taken, and provide it with all details regarding the frozen Funds, or any procedures taken, including attempted transactions
5. Notify the Section, if a former Customer, or occasional one, is a Designated Customer in the Sanctions List or the Local List.
6. Notify the Section of not taking any procedures, due to similarity in names, and this similarity in names was failed to be de-listed throughout the accessible and available information
7. DNFBPs shall de-freeze within Five working Days as of the date de-freezing order was issued by the Office. They also, need to provide the Section with the information related to the Funds, including its status, nature, value and the measures were taken and any other information related to the decisions.

And in all cases, DNFBPs shall immediately implement the Office's issuances regarding the implementation of UNSCRs under Chapter VII of the UN Convention concerning the Prevention and Suppression of terrorism and terrorism financing, and proliferation and its financing, and other relevant resolutions

## **Section Five**

### **Compliance Officer**

#### **Article (25)**

#### **Appointing Compliance Officer**

DNFBPs shall have to appoint compliance officer under their responsibilities to perform the functions set out in the By-Law and this Decision.

Appointment of compliance officer shall be under the following conditions:

- 1- Compliance officer shall not be younger than 21 years old
- 2- Compliance officer shall have an Education Qualification from an approved University or Higher Education Institute in the State or an equivalent so.
- 3- Compliance officer shall have the appropriate efficiency and expertise
- 4- Compliance officer shall be fully eligible and of good conduct, with good reputation, and no criminal record whether convicted in a crime, felony or misdemeanor related to honesty or trust, or whether was under disciplinary judgement in any of those crimes.

And in all cases, a prior written consent shall be obtained before appointing the compliance officer.

## **Article (26)**

### **Functions of Compliance Officer**

Compliance officer shall do the following functions:

- 1- Detect Transactions relating to Crime.
- 2- Review, scrutinize and study records, receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality.
- 3- Review the internal rules and procedures relating to combating the Anti-Money Laundering and their consistency with the Decree by Law, its By-Law and the present Decision
- 4- Assess the extent to which the institution is committed to the application of these rules and procedures, propose what is needed to update and develop these rules and procedures
- 5- Prepare and submit semi-annual reports on these points to senior management, and send a copy of that report to the relevant Supervisory Authority enclosed with senior management remarks and decisions.
- 6- Prepare, execute and document ongoing training and development programs and plans for the employees on Money Laundering and the means to combat them.
- 7- Collaborate with the Supervisory Authority and FIU, provide them with all requested data, and allow their authorized employees to view the necessary records and documents that will allow them to perform their duties.

## **Section Six**

### **Suspicious Transactions Reports (STRs)**

## **Article (27)**

### **Reporting using Suspicious Transactions Report**

If DNFBPs have reasonable grounds to suspect that a Transaction, attempted Transaction, or Funds constitute Crime Proceeds in whole or in part, or are related to the Crime or intended to be used in such activity, regardless of the amount, they shall adhere to the following without invoking bank secrecy or professional or contractual secrecy:

- A. Fill the STRs on Template (2) attached herewith.
- B. Directly report STRs to the FIU without any delay, via the electronic system of the FIU or by any other means approved by the FIU and provide them with the STR outlined in Clause (A).
- C. Respond to all additional information requested by the FIU.

### **Article (28)**

#### **Prohibition of Disclosing the Reporting Process**

- 1- DNFBPs, their staff, shall not disclose, directly or indirectly, to the Customer or any other person(s) that they have reported, or are intending to report a Suspicious Transaction, nor shall they disclose the information or data contained therein, or that an investigation is being conducted in that regard.
- 2- When DNFBPs attempt to discourage their Customers from committing a violation, they shall not be considered to have made a disclosure.

### **Section Four**

#### **Internal Supervision**

### **Article (29)**

DNFBPs shall have internal policies, procedures and controls for combating the Crime, that should be commensurate with the Crime risks, and with the nature and size of their business, and to continuously update them, including the following:

- 1- CDD measures towards Customers as required in accordance with the Decretal-Law, its By-Law and the present Decision, including procedures for the risk management of Business Relationships prior to completing the verification process.
- 2- put in place indicators that can be used to identify the suspicion on the occurrence of the Crime in order to report STRs, and shall update these indicators on an ongoing basis, as required, in accordance with the development and diversity of the methods used for committing such crimes, whilst complying with what the Supervisory Authorities or FIU may issue instructions in this regard.
- 3- Procedures for the reporting of Suspicious Transactions.

- 4- Appropriate arrangements for compliance management for combating the Crime, including appointing a compliance officer
- 5- Screening procedures to ensure the availability of high competence and compatibility standards when hiring staff
- 6- An independent audit function to test the effectiveness and adequacy of internal polices, controls and procedures relating to combating the Crime.

## **Section Eight**

### **Training Programs**

#### **Article (30)**

DNFBPs, throughout their compliance officer shall train their staff, taken into consideration the following:

1. Prepare and execute ongoing training programs to increase the level competency in adhering to regulations related to Money Laundering.
2. Taking into consideration to include methods of Money Laundering, how to discover and report them.
3. Coordinate about the scientific and applied materials for the training programs with the Committee, which the latter, shall have the right to give its opinions thereon and suggest these materials in light of any updates on the domestic, regional and international level.
4. Obligation to Keep records regarding all training programs that have been conducted within no less than five years, provided that it includes names of trainers, their qualifications and the subjects of those courses.

## **Section Nine**

### **Requirements related to New Technologies**

#### **Article (31)**

DNFBPs shall be updated about new technologies in the field of money laundering and, in particular, they should do the following:

1. Identify and assess the risks of money laundering that may arise when developing new products and new professional practices, including means of providing new services and using new or under-development techniques for both new and existing products.
2. Assess risks prior to the release of products, practices or techniques, and take appropriate measures to manage and mitigate such risks.

## **Section Ten**

### **Establishing Records and making Data Available**

#### **Article (32)**

##### **Establishing Records**

DNFBPs shall adhere to establish customers records that include the following:

1. All records, documents, data and statistics for all financial transactions and local or international commercial and cash transactions.
2. All records and documents obtained through CDD measures, ongoing monitoring, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed.
3. The records, documents and documents kept shall be organized so as to permit data analysis and tracking of financial transactions.

#### **Article (33)**

##### **Record Keeping**

DNFBPs shall keep such records for a period of no less than five years from the date of termination of the business relationship or from the closing date of the account to Customers who maintain accounts with these institutions or after the completion of a casual transaction or from the date of completion of the inspection by the Supervisory authorities, or from the date of issuance of a final judgment of the competent judicial authorities, all depending on the circumstances.

#### **Article (34)**

##### **Making all Information and Records Available**

DNFBPs shall make all Customer information regarding CDD towards Customers, ongoing monitoring and results of their analysis, records, files, documents, correspondence and forms available immediately to the competent authorities upon request.

## **Chapter Four**

### **Administrative Sanctions and Grievance**

#### **Article (35)**

##### **Procedures and Guarantees**

In case DNFBPs or their staff violated any provisions of the Decree by Law, its By-law or this decision, the Section shall notify them with the violation committed, and the violator shall submit an opposition response with all documents within 5 five working days from the date of the notification.

The Section shall submit a report to the Undersecretary after the expiration date along with the violation and response- if any, and their proposal thereto.

#### **Article (36)**

##### **Administrative Sanctions**

In case the violation was proven correct, the Undersecretary shall have the right to issue an order to impose administrative sanction upon the violator, with any of the following administrative sanctions:

- A. Warning
- B. Administrative Fine of not less than (AED 50,000) and not exceeding (AED 5,000,000) for each violation committed.
- C. Prohibiting the violator from conducting business in the sector where the violation occurred for a period of time outlined in the order.
- D. Restrict the powers of the Board of Directors whom are proven to have committed the violation, and the order may include the appointment of a temporary supervisor.
- E. Suspend those proven responsible for the violation, for a period of time set out in the order, or requesting substituting them if permissible.
- F. Seize or restrict conduct of business for the period set out in the order.
- G. Revocation of license

Except for clause (G), the Undersecretary shall have the right to request regular reports about the measures taken to correct the violation upon the imposition of administrative sanctions.

## **Article (37)**

### **Notification and publishing Administrative sanctions**

The Section shall be responsible for notifying DNFBPs about the order of sanction within 15 days from the date be it issued, by announcer in accordance to the procedures and methods stipulated in the Federal Law No. (11) of 1992 on Civil Procedures, its amendments and other related decision in implementation thereto.

The Section may publish its administrative sanctions in the different Media platforms.

## **Article (38)**

### **Grievances against the Administrative Sanctions**

DNFBPs may contest to the Minister about the administrative sanction within 15 days from the date be them notified or came to their knowledge. The Minister's decision in the contest shall be final. Not responding to the contest within 15 days from the date of submittal shall mean rejection of the contest.

The challenge against the administrative sanction decision shall not be accepted before contest thereon or after having the period for response passed, in accordance with Para. 1 of this Article

## **Chapter Five**

### **General concluding Provisions**

## **Article (39)**

### **Judicial Impoundment**

Section's Staff determined by virtue of decision from the Minister shall bear the capacity of Judicial Impoundment Officers and their role is to prove actions that violate the provisions of this Decretal Law, its By-Law and this present Decision.



#### **Article (40)**

##### **Professional Duties**

Obligations of BNFBPs as per the provisions of the Decretal Law, its By-law and this present Decision shall be considered professional duties, and any violation thereof shall be the liability of the violator without prejudice to Article (36) of this Decision.

#### **Article (41)**

##### **Publish and Enforceability**

This Decision shall be published in the Official Gazette and shall come into force as of the day be it published.

Sultan Saaed Al Baadi

The Minister of Justice