Decree 76/2022 of 2 March 2022 on adoption of the Regulation of Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing

Preamble

Law 37/2021 has amended Law 14/2017, of 22 June on the prevention and fight against money laundering and terrorist financing in order to incorporate in the Andorran legal system the provisions of Directive (EU) 2018/843 of the European Parliament and of the Council, of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU - 5th Directive -.

Law 37/2021 has also approved the relevant legal amendments - article 41 of Law 14/2017 - to transpose the Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk.

The complete transposition of these provisions in accordance to the commitments given to transpose regulations pursuant to the Monetary Agreement between the Principality of Andorra and the European Union, requires the amendment of the Regulation developing Law 14/2017, of 22 June on the prevention and fight against money laundering and terrorist financing, approved by Decree of 23 May 2018.

The amendment of the Regulation developing Law 14/2017 transposes EU legislation that regulates measures exclusively applicable to credit and financial institutions. Consequently, the scope of the new regulatory measures is limited to the financial parties under obligation with worldwide presence. Article 41 of Law 14/2017 establishes that financial parties under obligation that are part of a group shall implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group, for prevention of and fight against money laundering and terrorist financing purposes. Paragraph 4 of this article lays down that, where the law of the other country does not permit the implementation of the policies and procedures required, the financial parties under obligation shall ensure that branches and majority-owned subsidiaries in that country apply additional measures to effectively handle the risk and inform the UIFAND. This Decree approves the regulation of the additional measures for financial parties under obligation with branches or majority-subsidiaries, in the cases established in section 4 of article 41 of Law 14/2017.

In order to implement the aforementioned modification, the Regulation approved by means of this Decree combines the aforementioned provisions in a single regulatory text with the provisions contained in the Regulation implementing Law 14/2017, of 22 June, on the prevention and fight against money laundering and the financing of terrorism, approved by Decree of 23 May 2018, which is repealed.

This Regulation is formed by 29 articles.

Chapter one contains general provisions and specifies the scope of the definition of “politically exposed person” (PEP).

Chapter two establishes the minimum criteria to be considered by a reporting entity when carrying out its individual risk assessment and when determining its overall risk level, as well as the appropriate measures for the mitigation of these risks.

Chapter three develops the due diligence obligations of the reporting entities: identification of the customer, verification of the identity of the customer and of the latter's beneficial owner, simplified due diligence measures and enhanced due diligence measures.

Chapter four regulates the reporting obligations of the reporting entities and, in particular, the suspicious transaction report (STR) and its minimum content, the prohibition of disclosure and the freeze of transactions by UIFAND.

Chapter five specifies the internal control measures with which the reporting entities should provide themselves and, in particular, it develops the regulatory provisions on the internal audit function, internal policies and control procedures, and the training of reporting entities and of their personnel.

Chapter six establishes additional measures for financial parties under obligation with branches or majority-owned subsidiaries in other countries that do not allow the application of group policies and procedures.

Chapter seven contains various provisions on the actions of UIFAND; on the security, confidentiality and management of information by UIFAND; and on the relation between the provisions of the Regulation and the sanctioning regime of the Law.

At the proposal of the Minister of Finance the Government, at its session of 2 March 2022,

ENACTS

Sole Article

The Implementing Regulation of Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing is approved.

Repeal provision. Repeal of the Regulation of Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing

The implementing Regulation of Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing, approved by Decree of 23 May 2018 is repealed.

Sole final provision. Entry into force

1. This Regulation shall enter into force the day after of its publication in the Official Gazette of the Principality of Andorra (BOPA).

2. Notwithstanding the provisions of paragraph 1, the provisions established in the sixth chapter on additional measures for financial parties under obligation with branches or majority-subsidiaries in other countries that do not allow the application of group policies and procedures shall be applied within three months of their publication in the Official Gazette of the Principality of Andorra (BOPA).

Implementing Regulation of Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing.

Chapter One. General provisions

Article 1. Scope of application

The purpose of this Regulation is to develop the precepts established by Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing.

Article 2. Politically exposed persons

1. For the effects of what is provided in Letter h, Paragraph 6, Article 3 of the Law, the status of members of the administrative, management or supervisory bodies of parapublic entities, autonomous bodies and State-owned enterprises is held by the members of the administration body, the members of the general management or other equivalent officers.

2. For the purposes of what is provided in Paragraph 8, Article 3 of the Law, the profile required for the effects of the status of persons recognized as related is understood to exist when the relation with the related person is a matter of public knowledge or when the reporting entity is acquainted with or should be acquainted with the existence of such relation.

Chapter Two. Risk evaluation by reporting entities

Article 3. Individual risk assessment (IRA)

1. In application of Article 5 of the Law, when reporting entities identify and evaluate their risks of money laundering and of terrorist financing they should consider, among others, the following risk factors:

a) the nature, diversity and complexity of their businesses;

b) their target markets;

c) the number of customers and beneficial owners already identified as being of high risk;

d) the jurisdictions to which the reporting entity is exposed, either through its own activity or through the activities of its customers and beneficial owners, especially including the jurisdictions with high levels of corruption or of organized crime, and/or deficiencies in the controls for the fight against money laundering and terrorist financing identified by the Financial Action Task Force (FATF);

e) the distribution channels, including the way in which the reporting entity deals with its customers, the level of dependence on third persons for the performance of the due diligence measures and for the use of technology;

f) the results of the internal audit, as appropriate;

g) the volume and the size of their transactions, considering the customary activity of the respective reporting entity and the profile of its customers;

h) the products and services;

i) the monetary flows with each jurisdiction with which the reporting entity operates, in both the sphere of its own activity and in the sphere of the activities of its customers and beneficial owners;

j) the typology of enterprises or entities;

k) the legal structures or entities managed by lawyers, administrative service providers ("gestors") and/or professional providers of services to enterprises and trusts;

l) the legal structures or entities without apparent economic activity.

2. Reporting entities may supplement this information with information obtained from other significant internal or external sources such as business managers, personal account managers, national risk assessments, lists published by intergovernmental organizations or national governments, evaluation reports or reports on typologies of money laundering or of terrorist financing published by FATF or equivalent bodies such as Moneyval.

3. The individual risk assessment should be approved by the administration body and it constitutes the basis for the performance of the policies and the procedures aimed to mitigate the risks of money laundering and of terrorist financing because it reflects the risk profile of the reporting entity and determines its tolerance level. The policies, procedures, measures and controls for the mitigation of risks should be consistent with the individual risk assessment.

Article 4. Customer risk category

1. Reporting entities appropriately categorize the customer risk on the basis of the nature and size of the customer's business and the type of money laundering and terrorist financing risks to which the latter is exposed. Reporting entities categorizes the risk as high, medium or low or in any other way which suitably identifies the various risk categories.

2. On the basis of the information obtained in the application of the due diligence measures, reporting entities prepare the customer risk profile. This profile determines the level and type of continuous follow-up measures and provides support for the decisions relating to business relations.

3. The presence of isolated risk factors does not determine that the business relation is of higher-than-average risk. The reporting entity should duly justify it.

4. In the case of financial reporting entities, the customer risk profiles may be prepared individually or jointly when the customers show uniform characteristics such as, for example, customers with similar incomes or customers who carry out the same type of financial transactions.

Chapter Three. Due diligence obligations

Article 5. Occasional operations or transactions

For the effects of what is provided in Articles 8, 10 and 37 of the Law, an occasional operation or transaction is understood to be an operation which is not carried out as part of a business relation which has or seeks to have a certain duration.

Article 6. Identification of the customer and of the beneficial owner

1. Reporting entities identify customers and their beneficial owners in the terms provided in Article 9 of the Law, and take reasonable measures aimed to understand their ownership and control structure.

2. In the case of enterprises and entities in the process of being organized or incorporated, the identification should refer to the applicant natural person or persons. No other transactions may be made than the payments and debits derived from the incorporation or organization of the enterprise or of the entity until same is legally organized or incorporated and all the documents required by the Law and by this Regulation have been provided. Moreover, Andorran and foreign associations which have their headquarters in Andorra or which carry out activities on Andorran territory should be duly registered in the Register of Associations.

3. In the case of mutuals, associative entities, cooperatives and welfare funds, the persons who exercise the control of or who have a significant influence on the assets of the organization should be identified.

4. In the case of non-profit charitable organizations, clubs and associations, the necessary measures should be taken to identify at least two principal persons in charge or attorneys-infact and the identity of the institution itself. For the effects of this identification, principal persons in charge are considered to be the persons who exercise the control of or who have a significant influence on the assets of the organization, such as the members of a governing body or committee, the president, the members of the board and the treasurer.

Article 7. Verification of the identity of the customer and of the beneficial owner

1. In application of Letters a and b, Paragraph 1, Article 9 of the Law, reporting entities should take reasonable measures to verify the identity of customers and of their beneficial owners on the basis of documents, data or information obtained from reliable independent sources such as those specified in the following paragraphs of this article.

2. In the case of customers who are natural persons and beneficial owners, reporting entities should verify their identity by means, at least, of the display and copying of the official identity document bearing a photograph. Reporting entities may accept a copy of the identity document authenticated by a notary with the respective apostille, as appropriate.

When any person states that he acts on behalf of the customer, such circumstance should be verified by obtaining a copy of the respective power of attorney.

3. In the case of customers who are legal entities, trusts and other entities, reporting entities should identify the customer and the beneficial owner and verify their identity by means of the following documents, data or information:

a) Name or trade name, legal form, and proof of their existence. The verification may be made by means, among other documents, of an incorporation deed, the last annual report and annual accounts approved and deposited in a public register, a certificate of effectiveness issued by the respective register of companies, the instrument of constitution or some other documentation from a source equivalent to the aforementioned, which substantiates the name or trade name, legal form, and current existence of the customer.

b) Documents that substantiate the powers of representation of the person who acts on behalf of the legal entity, trust or entity. Reporting entities should also identify and verify the identity of such natural person.

c) Documents that regulate the internal regime of legal entities, trusts and other entities, such as the deed of incorporation or the articles of association of an enterprise, and the names of the persons who hold directive positions in the legal entity, trust or other entity.

d) The address of its registered office and, if it is different, the address of its main establishment or operation. The address should be verified through an information agency or by other means.

4. Financial reporting entities who maintain comprehensive or omnibus accounts of which the title is held by entities which are duly authorized to manage and to safeguard financial instruments or cash of their customers do not need to apply the measures of identification and verification which are required under Letters and a and b, Paragraph 1, Article 9 of the Law to the customers of the entity which is the title holder of the account in the case in which they operate through the comprehensive or omnibus account as long as:

- the entity holding the title to the account is an entity authorized to operate in the Principality of Andorra and the title to the account cannot lead to confusion, under any circumstances, with respect to the fact that the beneficial owners of the account are the customers of the entity holding the title to the account, or

- the entity holding the title to the account is an entity that is duly authorized to manage and to safeguard financial instruments or cash of its customers in a jurisdiction that is subject to standards on financial regulation and supervision and on matters of money laundering and terrorist financing equivalent to those in force in Andorra; and the title to the account cannot lead to confusion, under any circumstances, with respect to the fact that the beneficial owners of the account are the customers of the entity holding the title to the account.

It is considered that a jurisdiction is subject to standards on financial regulation and supervision and on matters of money laundering and terrorist financing equivalent to those in force in Andorra if, according to reliable independent sources such as, for example, reports of international bodies, it has an effective framework of financial regulation and supervision.

In this case, the reporting entity should collect sufficient information to understand and to determine reasonably the degree of equivalence of the regulatory and supervisory framework and of the framework in matters of money laundering and terrorist financing, especially in relation to the quality of its supervision and of the measures for protection of the assets of its customers.

In either case, financial reporting entities which maintain comprehensive or omnibus accounts should:

a) Obtain information relating to the territorial scope of the beneficial owners of the account, and to activities and products linked to the omnibus account.

b) Collect sufficient information to understand the nature of the activity and to determine the risk profile of the entity, as well as to determine reasonably, on the basis of information in the public domain, whether it has been subject to an investigation or to any other administrative or judicial action relating to the prevention of money laundering or terrorist financing.

c) Evaluate that the policies, procedures and internal controls of the entity holding the title to the account are suitable and effective for maintaining all the records and accounts which are

necessary to allow the assets of each customer and the entity's own assets to be distinguished at any time and without delay.

d) Evaluate that the policies, procedures and internal controls which the entity which holds the title to the account possesses for the prevention of money laundering and terrorist financing are suitable and effective.

e) Ensure that the entity which is the holder of the title to the account is in a position to identify and verify the identity of the beneficial owners of the assets deposited in the account.

f) Determine the level of risk which is entailed by the comprehensive or omnibus account, according to the information obtained and analysed, in matters of money laundering and terrorist financing.

g) Establish a procedure by means of which the entity which is the holder of the title to the account should immediately inform the financial reporting entity with respect to any intention to significantly change the use of the comprehensive or omnibus account. The financial reporting entity reserves the right to refuse the use of the account in support of any new commercial activity.

h) Obtain the authorization of the top management before opening the account and inform, at least every three months, its Board of Directors with respect to all the existing omnibus accounts, specifying the ones which have been newly opened during the period of reference.

i) Make periodic reviews with a focus on the risks of the entities which hold the title to these omnibus accounts in order to ensure that the requirements established above are continuously effective.

Article 8. Follow-up of business relations

1. In application of Paragraph 1.d , Article 9 of the Law, reporting entities request the necessary documents to justify the transaction or service requested by the customer when, on the basis of the amount, the terms of performance or any other characteristic of similar importance, such transaction or such service is not in accord with the usual activity, with the operational background, with the corporate purpose or with the knowledge that the reporting entity has of the customer.

2. In particular, reporting entities request this documentation in the following situations:

a) when the customer carries out or requests a transaction or a service for a very large amount with respect to its customary transactions;

b) when there is a substantial change in the customary functioning of the account; or

c) in other situations in which the reporting entity so deems necessary, on the basis of the risk analysis of the transaction.

Article 9. Simplified due diligence measures

1. Reporting entities may apply, among others, the following simplified due diligence measures in the cases in which the business relation or the occasional transaction shows a low degree of risk on the basis of the factors referred to in Paragraph 1, Article 11 of the Law:

a) Adjustment of the amount of information obtained for identification, verification of identity, or follow-up, among others,

i) on the basis of information obtained from a single document or from a single reliable, credible and independent source of information, or

ii) assuming the envisaged nature and purpose of the business relation to the extent in which the product is designed for a single particular use.

b) Reduction of the required information on the envisaged nature and purpose of the business relation and the scrutiny of the transactions when the risk associated with all the aspects of the business relation is low, on the basis of the source of the funds. It is considered that the risk is low, among other cases, when the funds are public monies.

c) Adjustment of the frequency of updates of the due diligence measures and the review of the business relation, for example carrying them out only when the customer wishes to subscribe a new product or service. Reporting entities should ensure, in all cases, that this adjustment does not result in a de facto exemption from the updating of the due diligence measures.

d) Adjustment of the frequency and intensity of the follow-up of transactions, for example when the transactions do not exceed a specific threshold. Reporting entities should ensure that the threshold is reasonable and that they have mechanisms for detecting related transactions that would exceed, as a whole, such threshold.

2. The information that reporting entities obtain when they apply simplified measures should be sufficient to consider that the analysis which determines that the risk is low is justified. Likewise, it should be sufficient to provide the reporting entity with sufficient information on the nature of the business relation so that it may detect any unusual or suspicious transaction. Simplified due diligence measures do not entail, in any case, that the reporting entity should not submit suspicious transaction reports.

3. Reporting entities do not apply simplified due diligence measures when there are suspicions of money laundering or terrorist financing, when there are doubts as to the truthfulness of the information obtained, or in any other scenario which the entity determines to be of high risk.

4. The identification of the shareholders or beneficial owners of listed enterprises or of the subsidiaries in which they have a majority interest is not required when such enterprises or subsidiaries are subject to information obligations which ensure the suitable transparency of their beneficial owner.

Article 10. Enhanced due diligence measures

1. The enhanced due diligence measures which reporting entities should apply in the cases referred to in Paragraph 1, Article 12 of the Law may include, among others, the following:

a) Increase of the volume of information obtained in the application of the due diligence measures with:

i) information on the customer and its beneficial owner, or the ownership and control structure, so that the risk associated with the business relation will be clearly understood. This requirement implies obtaining and evaluating information on the reputation of the customer and its beneficial owner. This information comprises the following data, among others:

- information on family relations and affinitive persons;

- information on present and past economic activities;

- adverse information that has appeared in the communication media.

ii) information on the envisaged nature of the business relation. This information supplements the risk profile of the customer and includes, among other data, the following:

- in the case of financial reporting entities: name, size and frequency of the transactions that they perform through the account, in order to allow detection of deviations which may give rise to suspicions, and to request justification;

- reasons for which the customer wishes a specific product or service, particularly when it is clear that the customer's needs can be filled in some other way or in a different jurisdiction;

- destination of the funds;

- nature of the business of the customer and of the beneficial owner, in order to allow the reporting entity to better understand the nature of the business relation.

b) Increase of the sources of information obtained in the application of the due diligence measures in order to verify the identity of the customer or of its beneficial owner by:

i) requiring that the first payment should be made through an account in the customer's name in a financial entity subject to due diligence standards equivalent to those established in Chapter Two of the Law.

ii) verifying that the origin of the assets and of the funds of the customer are consistent with the knowledge that the reporting entity has of the customer and of the purpose and the nature of the business relation. The verification of the origin of the assets or of the funds may be carried out, among other means, with tax returns (value added tax, personal income tax, wealth tax, corporation tax, other informative returns), copies of audited accounts, payrolls, public documents or reports from independent media.

c) Increase of the frequency of reviews in order to confirm that the risk associated with the business relation and the customer's profile continue to be in accord with the level of risk tolerated by the entity, or to identify transactions that require a subsequent review, with the performance of the following actions:

i) determination of whether the customer's risk profile has changed and the measure in which the risk can be kept under control.

ii) verification that any change in the customer's risk profile is identified, evaluated and, when appropriate, adjusted.

iii) Identification of any unusual or unexpected transaction that gives rise to a suspicion of money laundering or terrorist financing. This control involves the determination of the destination of the funds or of the reasons for specific transactions.

d) Procurement of the authorization of the top management to establish or to continue the business relation.

Reporting entities are not required to apply all the measures listed in this paragraph. Reporting entities should evaluate the application of the most appropriate measure or measures according to the evaluation of the risk.

2. Reporting entities evaluate the risk determined by the application of enhanced due diligence measures and leave a written record of their evaluation, which should be at the disposal of UIFAND, other competent supervisory authorities, external auditors and internal control and communication bodies.

3. When UIFAND detects that a specific product, customer, sector or territory poses a high risk of money laundering, it may instruct reporting entities, by means of a technical communiqué, to adopt the measures which it deems appropriate, including the following, among others:

a) prohibition of operating with same;

b) limitation of commercial relations or financial transactions with specific persons or territories;

c) enhancement of declaration mechanisms or establishment of special declaration procedures.

Chapter Four. Information obligations

Article 11. Reporting obligation

1. The reports to UIFAND which are established in Article 20 of the Law are also to be made with respect to transactions which have already been performed when, after the performance of the respective transaction, there are suspicions that it could constitute a transaction of money laundering or of terrorist financing.

2. Reports are always to be made in writing, on paper, and in the case of urgency they are to be made previously though any available medium, transmitting the subsequent written report within a maximum time of two working days. In such case, the written report should make reference to the previous initial communication and to the medium used for such communication.

3. As an exception to what is provided in the foregoing paragraph, UIFAND may set up secure telematic channels for the reporting entities to submit the respective suspicious transaction reports by such means.

Article 12. Content of the suspicious transaction report

1. In application of Article 20 of the Law, the suspicious transaction report should be accompanied, as a minimum, by the following information:

a) list and identification of the natural persons or legal entities and their beneficial owners who take part in the transaction, as well as the concept of their participation in such transaction;

b) list of the transactions, specifying date, purpose, currency, amount, and method and place or places of performance;

c) copy of the documentation by which identification has been made of the customer who has requested the performance of the suspicious transaction and, when appropriate, copy of the documentation by which identification has been made of the beneficial owner;

d) copy of the documentation by means of which the customer has justified the transaction;

e) statement of all the circumstances of the suspicious transaction which are known to the reporting entity.

2. In the event in which the reporting entity does not possess any of the aforementioned information items, it should so state expressly.

3. Subsequently to the suspicious transaction report, the reporting entity should convey to UIFAND any new element relating to the report which were to come to its knowledge. This obligation ceases on the date on which UIFAND notifies the reporting entity of the shelving of the file or of the forwarding of the file to the competent judicial authorities. In the latter case the communication obligations go on to be governed by what is determined by the competent judicial authority in accordance with the applicable laws.

4. Without prejudice to the provisions of the foregoing paragraph, in the case of the shelving of the file the reporting entity continues to have the obligation to communicate to UIFAND any new transaction which, by virtue of its characteristics, may entail a risk of money laundering or of terrorist financing, in the general terms established by the Law and by this Regulation.

5. In the exercise of its competences, UIFAND may request clarifications or additional information which the reporting entity may possess.

6. UIFAND publishes on its website the suspicious transaction report form which reporting entities are to use.

Article 13. Exceptions to the prohibition of disclosure

1. Reporting entities should request preliminary authorization from UIFAND in the cases provided in Article 26 of the Law. UIFAND may publish a model of request for authorization on its website.

2. As regards the request for authorization to which reference is made in Paragraph 3, Article 26 of the Law, the reporting entity should inform UIFAND as to the countries in which it has branches and subsidiaries with majority interest, to which it wishes to convey information, and it should state the measures of effective application of the group internal procedures and policies to which reference is made in Article 41 of the Law. UIFAND should verify the reasonability of this effective application and verify that these countries set requirements equivalent to those established in Andorran law on matters of the fight against money laundering and terrorist financing.

3. As regards the requests for authorization to which reference is made in Paragraphs 4 and 5, Article 26 of the Law, the reporting entity should inform UIFAND as to the suspicious transaction report or reports which it is wished to convey. UIFAND should verify that the reporting entities of other countries set requirements which are equivalent to those established in Andorran law in matters of the fight against money laundering and terrorist financing.

4. Requests for authorization should be answered within a maximum time of fifteen days counting from the date of their submission to UIFAND. In the event of silence of UIFAND upon the lapse of the aforementioned time, the request made by the reporting entity will be understood to be denied.

5. For the purposes of what is provided in Paragraphs 2 and 3, it is considered that a country sets requirements that are equivalent to those established in Andorran law in matters of the

fight against money laundering and terrorist financing if, according to reliable independent sources, such as for example mutual evaluation or detailed evaluation reports or follow-up reports, such country possesses measures against money laundering and terrorist financing which are compatible with the FATF Recommendations and same effectively applies such measures.

6. UIFAND may evaluate other factors, in addition to the territorial factor, for the effects of the requested authorization in the cases provided in Paragraph 1.

Article 14. Freeze of transactions

1. The provisional freeze of transactions which UIFAND may order in application of Paragraph 5, Article 20 of the Law is communicated to reporting entities in writing.

2. With the time of duration of the freeze, reporting entities should not carry out any action in relation to the frozen transactions without the prior written consent of UIFAND, nor should they carry out any transaction linked to or relating to the suspicious transaction.

Chapter Five. Internal control measures in matters of money laundering and terrorist financing

Article 15. Internal control and communication bodies

1. The internal control and communication body, the designation of which is required by Paragraph 2, Article 40 of the Law, should verify the constant and effective compliance with the respective obligations by the entity, by its administrators, by its top management and by its personnel, in accordance with Andorran law on the prevention of and fight against money laundering and terrorist financing.

To this end, reporting entities should adopt the necessary measures to ensure that the aforementioned body possesses appropriate human, training-related, material, technical and organizational means to comply with its functions.

2. The internal control and communication body may be of single-person character or collegial and its members should comply, as a minimum, with the following preliminary requirements for their appointment:

- They should be designated by the governing body or by the general management.

- They should possess the necessary professionalism to carry out their functions with integrity.

- They should possess the experience, knowledge of the Andorran legislative framework in matters of the prevention of the laundering of capital and terrorist financing, availability, and authority within the entity as are necessary to carry out their functions within the internal control and communication body in an effective way.

- They should have the authority to propose, at their own initiative, to the top management, all the measures and means necessary to ensure compliance with and the effectiveness of the internal measures for the prevention of the laundering of capital and terrorist financing.

Notwithstanding the foregoing, the composition of the internal control and communication body should be adapted to the structure, the complexity and the size of the business.

3. The internal control and communication body should have immediate access to all the documentation relating to the identification of customers, to the rest of the documentation

relating to compliance with the due diligence obligations, to the records of the transactions, and to any other relevant information.

4. Reporting entities which are legal entities should convey in writing to UIFAND complete information on the structure of the internal control and communication body, and also the name of and the position held in the enterprise by the persons who form it. Reporting entities should inform UIFAND of any changes within the internal control and communication body within a maximum time of fifteen days.

UIFAND may propose to reporting entities measures which will help to improve the functioning of their internal bodies.

5. In the case of reporting entities belonging to a group, compliance with the obligations contained in this article may be made within the framework of the group.

Article 16. Internal auditing function

1. In application of Article 40 of the Law, financial reporting entities should establish internal auditing and control procedures to examine and to evaluate the suitability and the effectiveness of the systems, the internal control mechanisms and the measures of the entity; to formulate recommendations, and to verify compliance with same.

2. In the case of reporting entities belonging to a group, compliance with the obligations contained in this article may be achieved within the framework of the group.

Article 17. Internal controls and procedures

1. Reporting entities should establish in writing internal policies and control procedures in the following matters:

a) policy of admission of customers based on the assessment and management of risks;

b) due diligence with respect to the identification of the customer and of the beneficial owner;

c) procurement of information on and verification of the identity of the customer and of the beneficial owner;

d) measures of confidentiality, conservation of documents, and updating of data;

e) internal procedure and channel of communication of indicative evidence of possible suspicious transactions, to the internal communication and control body, and measures of confidentiality;

f) channel and procedure of communication of suspicious transactions to UIFAND;

g) specific independent and anonymous channel for communication of infringements at internal level as required by Article 91.3 of the Law;

h) suitable policies and procedures to ensure high ethical standards in the hiring of employees, executives and agents.

These internal policies and control procedures are prepared by taking into account the size of the business and they should allow the management and mitigation of the risks identified, either by the authorities or by the reporting entity.

The internal policies and control procedures are to be approved by the top management. In all cases, the internal policies should be approved by the administration body.

2. The reporting entities should approve in writing and should apply an express policy of admission of customers based on the assessment evaluation and management of risks, in the terms provided in Article 3 of this Regulation. This policy should include a description of the types of customers who could pose a high risk of money laundering or of terrorist financing in accordance with the criteria for establishing enhanced diligence measures contained in Article 12 of the Law. The customer admission policy should be gradual and enhanced precautions should be adopted with regard to customers who pose a higher-than-average risk.

3. As regards the channel and the procedure of communication of suspicious transactions to UIFAND, the guidelines issued in this respect by UIFAND should be followed. Moreover, the internal control and communication body should adopt suitable measures to safeguard the confidentiality of communications.

4. In application of the obligation to possess suitable procedures which is provided in Paragraph 3, Article 91 of the Law, the reporting entities have a specific independent and anonymous communication channel so that their employees or persons in a similar position and executives may communicate internal infringements of the rules on prevention of money laundering and terrorist financing, or infringements of the procedures approved by the reporting entities for making compliance with said rules.

The communications should be made to the internal control and communication body or, at the choice of the reporting entity, to another internal body for regulatory compliance with equivalent authority-related and operational requirements.

If the communication channel used by the reporting entity is addressed to another internal body for regulatory compliance, the control and communication body should have knowledge of it. In all cases, the internal control body or the body receiving the report should apply the procedures necessary to ensure confidentiality as well as the conservation of the respective medium and of its content.

5. Once the internal control and communication body has received a communication, it should immediately analyse or verify it in order to determine the relation of the communicated facts or transactions with money laundering or terrorist financing and it should appraise the submission of a suspicious transaction report to UIFAND in application of Article 20 of the Law.

6. The internal procedures should be communicated by the financial reporting entities to the branches, the subsidiaries with majority interest and the local offices located abroad whose purpose is commercial or financial transactions. UIFAND may propose, to reporting entities, corrective measures for such internal controls and procedures.

Article 18. Training of reporting entities and of their personnel

1. The measures to which reference is made in Article 42 of the Law include the organization of training plans and of special updating courses addressed to their employees in general and, specifically, to the personnel who hold the positions which, due to their characteristics, are suitable for detecting the facts or transactions which may be related to money laundering and

terrorist financing; these training plans and courses should qualify such employees to carry out such detection and to know how to proceed in such cases.

2. The training should cover, as a minimum, the following:

- the applicable law;

- the types of money laundering;

- the procedures established by the body for the prevention of the laundering of capital and terrorist financing.

This training should be adapted to the responsibility held by the respective employees.

3. For the purpose of improving the prevention of money laundering and terrorist financing in the international framework as well, financial reporting entities and the reporting entities included under Letters a and b, Paragraph 2, Article 2 of the Law may exchange information and experiences not subject to confidentiality in accordance with the respective legislative provisions, with other entities of the same group or with other reporting entities of the same legal entity or associative network who share a common ownership, management and supervision, when same are established in States which set requirements equivalent to those provided in this Law.

Chapter Six. Additional measures of financial parties under obligation with a branch or a majority-owned subsidiary in third countries that do not permit the application of group-wide policies and procedures

Article 19. Subject matter and scope

This Chapter lays down a set of additional measures, including minimum action, that financial subjects under obligation must take to effectively handle the money laundering and terrorist financing risk where a third country's law does not permit the implementation of group-wide policies and procedures at the level of branches or majority-owned subsidiaries that are part of the group and established in the third country, as referred to in article 41 of Law.

Article 20. General obligations for other countries

For each country where they have established a branch or they are a majority owner of a subsidiary, financial parties under obligation shall at least:

a) assess the money laundering and terrorist financing risk to their group, record that assessment, keep it up to date and retain it in order to be able to share it with the UIFAND;

b) ensure that the risk referred to in point (a) is reflected appropriately in their group-wide anti-money laundering and countering the financing of terrorism policies and procedures;

c) obtain senior management approval at group-level for the risk assessment referred to in point a) and for the group-wide anti-money laundering and countering the financing of terrorism policies and procedures referred to in point b);

d) provide targeted training to relevant staff members in the third country to enable them to identify money laundering and terrorist financing risk indicators, and ensure that the training is effective.

Article 21. Individual risk assessment

1. In accordance with paragraph 4 of article 41 of Law, where the other country's law prohibits or restricts the application of policies and procedures that are necessary to identify and assess adequately the money laundering and terrorist financing risk associated with a business relationship or occasional transaction due to restrictions on access to relevant customer and beneficial ownership information or restrictions on the use of such information for customer due diligence purposes, financial parties under obligation shall at least:

a) inform the UIFAND without undue delay and in any case no later than 28 calendar days after identifying the third country of the following:

i) the name of the other country concerned;

ii) how the implementation of the other country's law prohibits or restricts the application of policies and procedures that are necessary to identify and assess the money laundering and terrorist financing risk associated with a customer;

b) ensure that their branches or majority-owned subsidiaries that are established in the other country determine whether consent from their customers and, where applicable, their customers' beneficial owners, can be used to legally overcome restrictions or prohibitions referred to in point a) ii);

c) ensure that their branches or majority-owned subsidiaries that are established in the other country require their customers and, where applicable, their customers' beneficial owners, to give consent to overcome restrictions or prohibitions referred to in point a) ii) to the extent that this is compatible with the other country's law.

2. Where the consent referred to in point c) of paragraph 1 is not feasible, financial parties under obligation shall take additional measures as well as their standard anti-money laundering and countering the financing of terrorism measures, to manage the money laundering and terrorist financing.

Those additional measures shall include the additional measure set out in point c) of article 26 and one or more of the measures set out in points a), b), d), e) and f) of that article.

Where a financial party under obligation cannot effectively manage the money laundering and terrorist financing risk by applying the measures referred to in paragraphs 1 and 2, it shall:

a) ensure that the branch or majority-owned subsidiary terminates the business relationship;

b) ensure that the branch or majority-owned subsidiary not carry out the occasional transaction;

c) close down some or all of the operations provided by their branch and majority- owned subsidiary established in the other country.

3. Financial parties under obligation shall determine the extent of the additional measures referred to in paragraphs 2 on a risk-sensitive basis and be able to demonstrate to the UIFAND that the extent of additional measures is appropriate in view of the money laundering and terrorist financing risk.

Article 22. Customer data sharing and processing

1. Where another country's law prohibits or restricts the sharing or processing of customer data for anti-money laundering and countering the financing of terrorism purposes within the group, financial parties under obligation shall at least:

a) inform the UIFAND without undue delay and in any case no later than 28 days after identifying the third country of the following:

i) the name of the third country concerned;

ii) how the implementation of the other country's law prohibits or restricts the sharing or processing of customer data for anti-money laundering and countering the financing of terrorism purposes;

b) ensure that their branches or majority-owned subsidiaries that are established in the other country determine whether consent from their customers and, where applicable, their customers' beneficial owners, can be used to legally overcome restrictions or prohibitions referred to in point a) ii);

c) ensure that their branches or majority-owned subsidiaries that are established in the other country require their customers and, where applicable, their customers' beneficial owners, to provide consent to overcome restrictions or prohibitions referred to in point a)ii) to the extent that this is compatible with the third country's law.

2. In cases where consent referred to in point c) of paragraph 1 is not feasible, financial parties under obligation shall take additional measures as well as their standard anti-money laundering and countering the financing of terrorism measures to manage risk. These additional measures shall include the additional measure set out in point a) of article 26 or the additional measure set out in point c) of that Article. Where the money laundering and terrorist financing risk is sufficient to require further additional measures, financial parties under obligation shall apply one or more of the remaining additional measures set out in points a) to c) of article 26.

3. Where a financial party under obligation cannot effectively manage the money laundering and terrorist financing risk by applying the measures referred to in paragraphs 1 and 2, it shall close down some or all of the operations provided by their branch and majority-owned subsidiary established in the other country.

4. Financial parties under obligation shall determine the extent of the additional measures referred to in paragraphs 2 and 3 on a risk-sensitive basis and be able to demonstrate to the UIFAND that the extent of additional measures is appropriate in view of the risk of money laundering and terrorist financing.

Article 23. Disclosure of information related to suspicious transactions

1. Where the other country's law prohibits or restricts the sharing of information referred to in article 20 of Law between branches and majority-owned subsidiaries established in other countries and other entities within the same group, financial parties under obligation shall at least:

a) inform the UIFAND without undue delay and in any case no later than 28 days after identifying the third country of the following:

i) the name of the country concerned;

ii) how the implementation of the third country's law prohibits or restricts the sharing or processing of the content of information identified by a branch and majority-owned subsidiary established in another country with other entities in their group;

b) require the branch or majority-owned subsidiary to provide relevant information to the financial party's senior management so that it is able to assess the money laundering and terrorist financing risk associated with the operation of such a branch or majority-owned subsidiary and the impact this has on the group, such as:

i) the number of suspicious transactions reported within a set period;

ii) aggregated statistical data providing an overview of the circumstances that gave rise to suspicion.

2. Financial parties under obligation shall take additional measures as well as their standard anti-money laundering and countering the financing of terrorism measures and the measures referred to in paragraph 1 to manage risk.

Those additional measures shall include one or more of the additional measures set out in points a) to c) and g) to i) of article 26.

3. Where financial parties under obligation cannot effectively manage the money laundering and terrorist financing risk by applying the measures referred to in paragraphs 1 and 2, they shall close down some or all of the operations provided by their branch and majority-owned subsidiary established in the other country.

4. Financial parties under obligation shall determine the extent of the additional measures referred to in paragraphs 2 and 3 on a risk-sensitive basis and be able to demonstrate to the UIFAND that the extent of additional measures is appropriate in view of the risk of money laundering and terrorist financing.

Article 24. Transfer of customer data

Where the other country's law prohibits or restricts the transfer of data related to customers of a branch and majority-owned subsidiary, for the purpose of supervision for anti-money laundering and countering the financing of terrorism, financial parties under obligation shall at least:

a) inform the UIFAND without undue delay and in any case no later than 28 calendar days after identifying the other country of the following:

i) the name of the other country concerned;

ii) how the implementation of the other country's law prohibits or restricts the transfer of data related to customers for the purpose of supervision for anti-money laundering and countering the financing of terrorism;

b) carry out enhanced reviews, including, where this is commensurate with the money laundering and terrorist financing risk associated with the operation of the branch or majority-owned subsidiary established in the other country, onsite checks or independent audits, to be satisfied that the branch or majority-owned subsidiary effectively implements group-wide policies and procedures and that it adequately identifies, assesses and manages the money laundering and terrorist financing risks;

c) provide the findings of the reviews referred to in point b) to the UIFAND upon request;

d) require the branch or majority-owned subsidiary established in the other country to regularly provide relevant information to the financial party's senior management, including at least the following:

i) the number of high risk customers and aggregated statistical data providing an overview of the reasons why customers have been classified as high risk, such as politically exposed person status;

ii) the number of suspicious transactions identified and reported and aggregated statistical data providing an overview of the circumstances that gave rise to suspicion;

e) make the information referred to in point (d) available to the UIFAND upon request.

Article 25. Record-keeping

1.Where another country's law prohibits or restricts the application of record-keeping measures equivalent to those specified in Law, financial parties under obligation shall at least:

a) inform the UIFAND without undue delay and in any case no later than 28 days after identifying the other country of the following:

i) the name of the other country concerned;

ii) how the implementation of the other country's law prohibits or restricts the application of record-keeping measures equivalent to those laid down in Law;

b) establish whether the consent from the customer and, where applicable, their beneficial owner, can be used to legally overcome restrictions or prohibitions referred to in point a) ii);

c) ensure that their branches or majority-owned subsidiaries that are established in the other country require customers and, where applicable, their customers' beneficial owners, to provide consent to overcome restrictions or prohibitions referred to in point a) ii) to the extent that this is compatible with the third country's law.

2. In cases where consent referred to in point c) of paragraph 1 is not feasible, financial parties under obligation shall take additional measures as well as their standard anti-money laundering and countering the financing of terrorism measures and the measures referred to in paragraph 1 to manage risk. These additional measures shall include one or more of the additional measures set out in points a) to c) and j) of article 26.

3. Financial parties under obligation shall determine the extent of the additional measures referred to in paragraph 2 on a risk-sensitive basis and be able to demonstrate to the UIFAND that the extent of additional measures is appropriate in view of the risk of money laundering and terrorist financing.

Article 26. Additional measures

Financial parties under obligation shall take the following additional measures pursuant to article 21 (2), article 22(2), article 23(2) and article 25(2) respectively:

a) ensuring that their branches or majority-owned subsidiaries that are established in the other country restrict the nature and type of financial products and services provided by the branch of majority-owned subsidiary in the other country to those that present a low money laundering and terrorist financing risk and have a low impact on the group's risk exposure;

b) ensuring that other entities of the same group do not rely on customer due diligence measures carried out by a branch or majority-owned subsidiary established in the other country, but instead carry out customer due diligence on any customer of a branch or majority-owned subsidiary established in other country who wishes to be provided with products or services by those other entities of the same group even if the conditions in article 18.4 of Law are met;

c) carrying out enhanced reviews, including, where this is commensurate with the money laundering and terrorist financing risk associated with the operation of the branch or majority-owned subsidiary established in the other country, onsite checks or independent audits, to be satisfied that the branch or majority-owned subsidiary effectively identifies, assesses and manages the money laundering and terrorist financing risks;

d) ensuring that their branches or majority-owned subsidiaries that are established in the other country seek the approval of the financial party's senior management for the establishment and maintenance of higher-risk business relationships, or for carrying out a higher risk occasional transaction;

e) ensuring that their branches or majority-owned subsidiaries that are established in the other country determine the source and, where applicable, the destination of funds to be used in the business relationship or occasional transaction;

f) ensuring that their branches or majority-owned subsidiaries that are established in the other country carry out enhanced ongoing monitoring of the business relationship including enhanced transaction monitoring, until the branches or majority-owned subsidiaries are reasonably satisfied that they understand the money laundering and terrorist financing risk associated with the business relationship;

g) ensuring that their branches or majority-owned subsidiaries that are established in the other country share with the financial parties under obligation underlying suspicious transaction report information that gave rise to the knowledge, suspicion or reasonable grounds to suspect that money laundering and terrorist financing was being attempted or had occurred, such as facts, transactions, circumstances and documents upon which suspicions are based, including personal information to the extent that this is possible under the other country's law;

h) carrying out enhanced ongoing monitoring on any customer and, where applicable, beneficial owner of a customer of a branch or majority-owned subsidiary established in the other country who is known to have been the subject of suspicious transaction reports by other entities of the same group;

i) ensuring that their branches or majority-owned subsidiaries that are established in the other country has effective systems and controls in place to identify and report suspicious transactions;

j) ensuring that their branches or majority-owned subsidiaries that are established in the other country keep the risk profile and due diligence information related to a customer of a branch or majority-owned subsidiary established in the other country up to date and secure at least during a period of 5 years, and in any case for at least the duration of the business relationship.

Chapter Seven. Other provisions

Article 27. Actions of UIFAND

1. UIFAND should document, by means of written records, its actions within the framework of the on-site inspections carried out on the reporting entities in the exercise of the functions attributed to it by Article 55 of the Law.

2. In application of Paragraph 2.p, Article 55 of the Law, UIFAND prepares and publishes annually sufficient statistics to evaluate the effectiveness of the prevention of and the fight against money laundering and terrorist financing. Such statistics cover, as a minimum, the following data:

a) suspicious transaction reports and other reports received and conveyed, including the itemization by types of reporting entities;

b) actions of UIFAND relating to investigations on the prevention of and fight against money laundering and terrorist financing, denunciations received and freezes of transactions;

c) requests for international cooperation sent out by UIFAND or addressed to UIFAND;

d) other actions carried out by UIFAND.

Article 28. Security, confidentiality, protection and management of information by UIFAND
UIFAND adopts internal rules with instructions for its personnel on security, confidentiality and management of information within UIFAND. UIFAND applies suitable policies and procedures to ensure high standards of security in the hiring of employees.

Article 29. Sanctioning regime

The breach of the provisions of this Regulation will be sanctioned in accordance with the provisions of Chapter Twelve of the Law.

This Regulation is made public for its general knowledge.

Andorra la Vella, 2 March 2022

Xavier Espot Zamora

Head of Government