Consolidated version of Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing

Consolidated version of Law 14/2017, of 22 June, on the prevention and fight against money laundering and terrorist financing

Chapter I. General provisions.

Section 1. Subject-matter, scope and definitions

Article 1. Subject-matter

1. This Law aims to prevent and fight money laundering and terrorist financing.

2. For the purposes of this Law, the commission of any conduct so defined in the Criminal code shall be regarded as money laundering and terrorist financing.

Article 2. Parties under obligation

This Law shall apply to the following parties under obligation:

1. **Financial parties under obligation**, which are the natural or legal persons included in the following categories:
    a) operative entities of the financial system;
    b) insurance and reinsurance undertakings authorised to operate in the life insurance sector;
    c) insurance intermediaries (corredors d'assegurances), natural or legal persons who, for remuneration, pursues mediation within the life insurance sector;
    d) post office giro institutions;
    e) authorized payment service providers according to letters f) and h) of section 1 of article 4 of the Law on payment services and electronic money, with the exceptions provided by Regulations;
    f) virtual asset service providers.
2. The following **natural persons or legal entities**, **in the exercise of their professional activity:**
    a) auditors, external accountants and tax advisors, and any other person that undertakes to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters as their main business or professional activity;
    b) notaries, lawyers and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:
        - buying and selling or other disposition acts of real property or entities;
        - managing of client money, securities or other assets;
        - opening or management of bank, savings or securities accounts;
        - organisation of contributions necessary for the creation, operation or management of companies;
        - creation, operation or management of trusts, companies, associations, foundations, or similar structures;
    c) economists, administrative services managers, and other service providers to companies, other legal entities, trusts and other fiduciary arrangements;

d) real estate agents carrying out activities related to buying and selling properties, and also real estate agents when acting as intermediaries in the letting of immovable property, but only in relation to transactions for which the monthly rent amounts to EUR 10,000 or more;
e) persons trading in goods to the extent in which the payments are made or are received in cash for an amount equal to or greater than 10,000 euros or the equivalent value in foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
f) casinos and other providers of gambling services, on-site or online. By regulatory means, gambling that presents a low risk of money laundering and terrorist financing may be excluded totally or partly (except in the case of casinos), on the basis of a risk analysis using all relevant sources of information;
g) non-profit organizations under the terms established in the First Additional Provision of this Law. By regulatory means, the group of organizations which will be parties under obligation may be determined, on the basis of a risk analysis using all relevant sources of information, identifying the characteristics and type of organizations which, by virtue of their activities and particularities, are susceptible to be exposed to the risk of being used for purposes of terrorist financing;
h) trustees or persons who hold an equivalent position in legal structures similar to trusts in a non-professional way, under the terms established in the Third Additional Provision of this Law;
i) persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10,000 or more;
j) persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out in free zones, where the value of the transaction or a series of linked transactions amounts to EUR 10,000 or more;
k) managers of free zones and operators established therein.

3. **Non-resident natural and legal persons which carry out in the Principality of Andorra any activity of the same nature** as those listed in this article are subject to this Law. Its consideration as financial or non-financial parties under obligation is determined by the nature of the activity carried out

Article 3. Definitions

For the purposes of this Law, the following definitions apply:

1. **Funds**: those which are defined as such according to Article 366 bis of the Criminal Code.

2. **Self-regulatory body**: means a body that represents members of a profession and has a role in regulating them, performing certain supervisory or monitoring type functions and in ensuring the enforcement of the rules of their professions.

3. **Beneficial owner**: means any natural person(s) who ultimately controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

a) In the case of corporate entities:
   i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with international law which ensure adequate transparency of ownership information.
   A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25% in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership.
   The existence of «control by other means» may be determined, inter alia, in conformity with the criteria established in Law 30/2007, of 20 December, on the accounting of entrepreneurs.
   ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point i) is identified, or in if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who carry out the effective management through other means.
   iii) if no person under point i) and point ii) is identified, the natural person who acts as the chief executive officer or with equivalent executive powers.
   Parties under obligation shall keep records of the actions taken in order to identify the beneficial owner under points i), ii) and iii) aforementioned and shall be in a position to certify having used all means referred to in point ii).

b) In the case of trusts, all following persons:
   i) the settlor(s);
   ii) the trustee(s);
   iii) the protector(s), if any;
   iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity are yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
   v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

c) In the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point b).

4. **Service providers to companies and trust**: a natural person or legal entity who provides the following services to third parties:

a) the incorporation of companies or other legal entities;
b) acting as, or arranging for another person to act as, a director or secretary/attorney-in-fact/administrator of a company, a partner of a partnership, or a similar position in relation to other legal persons;

c) providing a registered office, business address or accommodation, correspondence or administrative address or other similar services for a company, a partnership or any other legal person or arrangement;
d) acting as, or arranging for another person to act as, a trustee of a trust or performing the equivalent function in other legal arrangements;
e) acting as, or arranging for another person to act as, a nominee shareholder for another person.

5. **Correspondent relationship** means:

a) the provision of banking services by one banking entity as the correspondent to another banking entity as the respondent, including, among others, providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;
b) the relationships between and among financial entities and banking entities and financial entities where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

6. **Politically exposed person**: means a natural person who is or who has been entrusted with prominent public functions and includes the followings:

a) heads of State, heads of government, ministers and deputy or assistant ministers;
b) consellers generals or members of similar national, foreign, international or supranational legislative bodies or any public assembly exercising legislative powers;
c) cònsols majors i menors (city mayors), finance and urban planning municipal councillors and equivalent positions in other countries;
d) members of the governing bodies of political parties;
e) members of the Superior Court of Justice (Andorran Supreme Court), of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
f) members of the Andorran Court of Auditors, of foreign courts of auditors, and members of the boards of central Banks or equivalent;
g) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
h) members of the administrative, management or supervisory bodies of para-public entities, autonomous bodies and State-owned enterprises;
i) directors, deputy directors and members of the board or equivalent functions of an international organisation.

Each international organisation accredited in Andorra shall issue and keep up to date a list of prominent public functions at the international organisation which shall be at the disposal of the UIFAND.

No public function referred to in points a) to i) shall be understood as covering middle-ranking or more junior officials;

7. **Familiar membres** includes the following:

a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
b) the children and their spouses, or persons considered to be equivalent to spouse, of a politically exposed person;
c) the parents of a politically exposed persons.

8. **Persons known to be close associaets** means:

a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any close business relations, with a politically exposed person;
b) natural person who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

9. **Tax advisor**: means any natural o legal person(s) that, exclusively or not, provide advice in tax matters.

10. **Management**: means an officer or employee with sufficient knowledge of the money laundering and terrorist financing exposure of the entity and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

11. **Senior management**: means senior management members in the terms established by article 2 of Law 8/2013, of 9 May, on the organisational requirements and functioning conditions of operative entities of the financial system, investor protection, market abuse and financial guarantee agreements.

12. **Business relationship**: means a business, professional or commercial relationship which is connected with the professional activities of a party under obligation and which is expected, at the time when the contact is established, to have an element of duration.

13. **Entities or parties under obligation of the same group:** means entities or parties under obligation that belong to a group pursuant to the definition laid down in article 34.2 of the consolidated text of Law 30/2007, of 20 December, on the accounting of entrepreneurs.

14. **Electronic money:** as defined in paragraph 16 of article 3 of Law 8/2018, of 17 May, on payment services and electronic money. This definition does not include the following:

i) monetary value stored on instruments referred to in letter k) of article 2 (3) of Law 8/2018;
ii) monetary value stored that is used to execute transactions referred to in letter l) of article 2 (3) of Law 8/2018.

15. **Shell bank:** means banking entities or financial entities, or an institution that carries out activities equivalent to those carried out by banking and financial entities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group under an effective supervision in the consolidated base.

For the purposes of this Law, physical presence means meaningful mind and management located in a country. The existence simply of a local agent or a reduced number of employees which is not proportionate to the activity or the nature of the business does not constitute physical presence.

16. **Cash:**

a) bearer-negotiable instruments including monetary instruments in bearer form such as travellers' cheques, negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery and incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted;
b) currency (banknotes and coins that are in circulation as a medium of exchange).
c) nominative cheques are not deemed to be cash.

17. **UIFAND**: Financial Intelligence Unit of Andorra, body configured as an administrative authority with functional autonomy that acts with independence from the rest of the General State Administration, in full respect of this Law and the legal system.

18. **Gambling services**: any service that involves bets of monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker and betting, which service is provided in a physical location, or by any remote means, by electronic means or by any other technology that facilitates communication, at the individual request of the recipient of the service.

19. **Non-profit organizations (NPOs):** a legal person or arrangement or organization, including associations and foundations, that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of good works.

20. **Virtual assets**: any digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.

21. **Virtual asset service providers**: any natural or legal person who as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i) exchange between virtual assets and fiat currencies;
ii) exchange between one or more forms of virtual assets;
iii) transfer of virtual assets;
iv) safekeeping or administration of virtual assets or instruments enabling control over virtual assets;
v) participation in and provision of financial services related to an issuer's offer or initial sale of a virtual asset.

Secction 2. Risk assessment

Article 4. Risk assessment by the authorities

1. The UIFAND coordinates the adoption of the appropriate national measures to identify, assess, understand and mitigate the risks of money laundering and terrorist financing. This evaluation is periodically reviewed and, particularly, when there are major events or developments.

2. After carrying out the risk assessment referred to in paragraph 1, competent authorities take the appropriate measures to:

a) prevent or mitigate money laundering and terrorist financing on a risk-based approach;
b) improve the national system of prevention and fight against money laundering and terrorist financing, in particular by identifying any areas where parties under obligation are to apply enhanced measures and, where appropriate, specifying the measures to be taken;
c) identify, where appropriate, sectors or areas of lower or greater risk of money laundering and terrorist financing;
d) allocate and prioritise the resources to combat money laundering and terrorist financing;
e) promote drafting appropriate rules for each sector or area, in accordance with the risks of money laundering and terrorist financing;
f) promote drafting appropriate rules for each sector or area, in accordance with the risks of money laundering and terrorist financing;
g) report, where applicable, to the appropriate national and international institutions and bodies, on the institutional structure and broad procedures of their AML/CFT regime, including, the UIFAND, the tax authorities and prosecutors, as well as the allocated human and financial resources to the extent that this information is available;
h) report, where applicable, to the appropriate national and international institutions and bodies on national efforts and resources (labour forces and budget) allocated to combat money laundering and terrorist financing.

3. For the purposes of contributing to the preparation of risk assessment, UIFAND may request the information deemed appropriate to maintain comprehensive statistics to identify and evaluate the risks of money laundering and terrorist financing and the effectiveness of the system.

These statistics include, among others:

a) data measuring the size and importance of the different sectors which fall within the scope of this Law, including the number of entities and persons and the economic importance of each sector;
b) data measuring the reporting, investigation and judicial phases of the national system of prevention and fight against money laundering and terrorist financing, including the number of suspicious transaction reports made to the UIFAND, the follow-up given to those reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences, the types of predicate offences, where such information is available, and the value in euro of property that has been frozen, seized or confiscated;
c) if available, data identifying the number and percentage of reports resulting in further investigation, together with the annual report to parties under obligation detailing the usefulness and follow-up of the reports they presented;

d) data regarding the number of cross-border requests for information that were made, received, refused and answered, partially or fully, by the UIFAND and other competent authorities, broken down by country;
e) human resources allocated to the UIFAND and Andorran Financial Authority to fulfil their tasks;
f) number of on-site and off-site supervisory actions, the number of breaches identified through supervisory actions and sanctions and administrative measures adopted by the UIFAND and other competent authorities.

4. The UIFAND shall report the results of the risk assessment to the relevant international bodies. The UIFAND shall make publicly available on the UIFAND website a summary of the assessment that shall not contain classified information.

Article 5. Risk assessment by the parties under obligation

1. Parties under obligation shall take appropriate steps to identify, assess and understand the risks of money laundering and terrorist financing. This individual risk assessment (ERI) shall:

a) be appropriately documented and reflected in a written report;
b) take into account all the relevant risk factors before determining the global level of risk and the appropriate mitigation measures. These risk factors shall include those relating to their customers, countries or geographic areas, products, services, transactions or delivery channel;
c) periodically reviewed and, particularly, when there are major events or developments in the management or activity of the party under obligation.

The UIFAND may issue guidelines on what are appropriate measures taking into account the nature and size of the parties under obligation.

2. The ERI shall be made immediately available to the UIFAND upon its request at any time.

3. The UIFAND may decide that the ERI is not required for certain sectors with limited risks where the specific risks inherent in the sector are clear and understood and parties under obligation, individually, understand their risks. The UIFAND communicates this circumstance to the parties under obligation.

Secció tercera. High-risk countries

Article 6. High-risk countries

1. The UIFAND identifies the countries with high-risk of money laundering and terrorist financing by means of a technical communiqué, taking into account the countries and jurisdictions designated by the Financial Action Task Force as non-cooperative or with strategic deficiencies and those considered by the European Commission to have strategic deficiencies in their national systems of prevention and fight against money laundering and terrorist financing.

2. Parties under obligation shall apply enhanced customer due diligence measures in business relationships and transactions related to natural and legal persons of high-risk countries.

3. The UIFAND may approve the application of countermeasures in relation to high-risk countries or countries with a high risk of money laundering and terrorist financing. These countermeasures may be adopted independently or according to any decision or recommendation of international organisations, institutions or groups.

Appropiate countermeaures include, among others:

a) Forcing parties under obligation to apply enhanced customer due diligence measures.
b) Implementing appropriate enhanced reporting mechanisms or the systemic reporting of certain transactions.
c) Prohibiting incorporating or maintaining subsidiaries, branches or representative offices of financial entities of the concerned country, or otherwise taking into account the fact that the concerned financial entity is from a country that does not have an adequate system of prevention and fight against money laundering and terrorist financing.
d) Prohibiting parties under obligation from incorporating or maintaining subsidiaries, branches or representative offices in the concerned country, or otherwise taking into account the fact that they are in a country that does not have an adequate system of prevention and fight against money laundering and terrorist financing.
e) Limiting, and even prohibiting, business relationships or financial transactions with the concerned country or natural and legal persons of that country.
f) Prohibiting parties under obligation from accepting the customer due diligence measures taken by the entities of the concerned country.
g) Requiring financial parties under obligation from reviewing, modifying or, where applicable, terminating the correspondent relationship with financial entities of the concerned country.
h) Carrying out enhanced supervision of subsidiaries and branches of financial entities of the concerned countries or subjecting them to an external audit.
i) Imposing enhanced external audit obligations on financial groups in relation to any subsidiary or branch located or operating in the concerned country.

Chapter II. Customer due diligence measures

Section 1. General provisions

Article 7. Prohibition of anonymous accounts, passbooks, safe-deposit boxes and payments carried out with prepaid cards

Accounts, passbooks and safe-deposit boxes with fictitious name or anonymous are prohibited.

Payments carried out by using anonymous prepaid cards are not accepted in the Andorran territory.

Article 8. Obligation to apply customer due diligence measures

Parties under obligation shall apply customer due diligence measures in the following circumstances:

a) when establishing a business relationship;
b) when carrying out an occasional transaction that:

i) amounts to EUR 15,000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or
ii) constitutes a wire transfer, as defined in article 29 of this Law, exceeding EUR 1,000;

c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
d) in the case of casinos and other providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
f) when there is a suspicion about the veracity, adequacy and validity of previously obtained customer identification data;
g) when such transactions are listed as susceptible to entail money laundering or terrorist financing or are qualified of special monitoring by the UIFAND by means of a technical communiqué;
h) in the case of virtual asset service providers, occasional transactions with a value of EUR 1,000 or more trigger the requirement to conduct customer due diligence measures.

Article 9. Scope of customer due diligence measures

1. Customer due diligence shall comprise:

a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means as set out in the Law on electronic trust services in force;
b) identifying the beneficial owner and taking reasonable measures to verify that person's identity, on basis of documents, data or information obtained from a reliable and independent source, so that the party under obligation is satisfied that it knows who the beneficial owner is. Additionally, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer.
Where the beneficial owner identified is the person who acts as a senior managing official or with equivalent executive powers as referred to in subsection (iii) of letter a) of paragraph 3 of article 3 of this Law, parties under obligation shall take the necessary reasonable measures to verify the identity of this natural person and shall keep records of the actions taken and any difficulties encountered during the verification process.
c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
d) conducting ongoing monitoring of the business relationship including:
- scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the party under obligation's knowledge of the customer, the business and risk profile, including the source of funds; and

- adopt measures to ensure that the documents, data or information held are kept up-to-date and are appropriate, verifying the existing documentation, especially for high-risk customers.

e) the assessment, understanding, and procurement of information to identify and to verify the origin of the funds which are the object of the business relationship or of the occasional transaction.

When performing the measures referred to in points a) and b), parties under obligation shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

2. The collected data shall be up-to-date so as to allow the correct identification of customers when establishing a business relationship or carrying out a transaction susceptible of entailing money laundering or terrorist financing.

3. Parties under obligation determine the extent of such customer due diligence measures on a risk-sensitive basis.

Parties under obligation take into account, among others, the following variables for assessing the risks of money laundering and terrorist financing:

a) the purpose of an account or business relationship;
b) the level of assets to be deposited by a customer or the size of transactions to be undertaken;
c) the regularity or duration of the business relationship.

In any case, parties under obligation should be able to prove to UIFAND that the customer due diligence measures which they have adopted are appropriate to the money laundering and terrorist financing risks which have been identified.

4. For life or other investment-related insurance business, in addition to the customer due diligence measures required in the previous sections, financial parties under obligation shall conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment-related insurance policies, as soon as the beneficiaries are identified or designated:

a) in the case of beneficiaries that are identified as specifically named persons or legal arrangements, taking the name of the person;
b) in the case of beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the baking entity or financial entity that it will be able to establish the identity of the beneficiary at the time of the payout.

The verification of the identity of the beneficiaries shall take place at the time of the payout. In the case of assignment, in whole or in part, of the life or other investment-related insurance to a third party, parties under obligation aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for its own benefit the value of the policy assigned.

Parties under obligation shall include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced customer due diligence measures are applicable. If the financial entity determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it should be required to take enhanced measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

5. In the case of beneficiaries of trusts or of similar legal arrangements that are designated by particular characteristics or class, a party under obligation shall obtain sufficient information concerning the beneficiary to satisfy the party under obligation that it will be able to establish the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

6. Parties under obligation shall conduct an ongoing monitoring as regards new technologies to avoid its undue use for money laundering or terrorist financing purposes and any other action causing a customer false identification in all non-face-to-face transactions.

Parties under obligation shall identify and assess the money laundering and terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Parties under obligation shall:

a) undertake the risk assessments prior to the launch or use of such products, practices and technologies; and
b) take appropriate measures to manage and mitigate the risks.

Article 10. Verification of the identity of customer and the beneficial owner

1. Els subjectes obligats verifiquen la identitat del client i del beneficiari efectiu abans que s'estableixi una relació de negocis o que es dugui a terme una operació.

Whenever entering into a new business relationship with a company or other legal entity, or a trust or a legal arrangement having a structure or functions similar to a trust, which are obliged to obtain, keep and provide information regarding the beneficial owners, parties under obligation shall collect proof of registration or an excerpt of the Registry.

2. By way of derogation from paragraph 1, verification of the identity of the customer and the beneficial owner may be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such situations, those procedures shall be completed as soon as practicable after initial contact.

3. By way of derogation from paragraph 1, an account within an operative entity of the financial system, including accounts that permit transactions in transferable securities, may be opened provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until the identification and the verification of the identity of the customer and the beneficial owner.

4. Where the identification of the customer and the beneficial owners, the verification of the its identity and the evaluation and the obtaining of information on the purpose and intended nature of the business relationship cannot be carried out according to article 9 of this Law or there are doubts about the veracity or adequacy of the information obtained, parties under obligation shall not establish a business relationship or carry out an occasional transaction. In the case of relationships that have already started, the business relationship shall be terminated.

In both cases, parties under obligation shall consider submitting a suspicious transaction report to the UIFAND.

5. Parties under obligation shall apply the customer due diligence measures at appropriate times to existing customers on the basis of risk analysis, or when the relevant circumstances of a customer change, or when the obliged entity has any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owners or in application of the obligations set out in Law 19/2016, of November 30, on the automatic exchange of information in tax matters.

6. In cases where parties under obligation form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the customer due diligence process will tip-off the customer, they are allowed not to pursue the customer due diligence process, provided that a suspicious transaction report is submitted to the UIFAND.

Section 2. Simplified customer due diligene measures.

Article 11. Simplified customer due diligence measures

1. Parties under obligation may apply simplified customer due diligence measures in those cases in which the business relationship or the transaction presents a low degree of risk according to the following factors:

1) Customer risk factors:
    a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
    b) public administrations or enterprises;
    c) customers resident in geographical areas of lower risk as set out in point 3).
2) Product, service, transaction or delivery channel risk factors:
    a) life insurance policies where the annual premium is no more than EUR 1,000 or the single premium is no more than EUR 2,500;
    b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
    c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
    d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).

3) Geographical risk factors - registration, establishment, residence in:
   a) European Union Member states;
   b) countries having effective systems of fight against money laundering and terrorist financing;
   c) countries identified by reliable and independent sources as having a low level of corruption or other criminal activity;
   d) countries which, on the basis of reliable and independent sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and effectively implement those measures.

The UIFAND may issue guidelines on the adoption of simplified customer due diligence measures which are appropriate and proportionate to the nature and size of the parties under obligation.

2. Before applying simplified customer due diligence measures, parties under obligation shall ascertain that the business relationship or the transaction presents a low degree of risk.

3. Parties under obligation carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

Section 3. Enhanced customer due diligene measures

Article 12. Enhanced customer due diligence measures

1. Els subjectes obligats apliquen mesures reforçades de diligència deguda en els següents casos:

a) cases referred to in article 12 bis to 17 of this Law;
b) transactions with natural or legal persons established in countries identified by the UIFAND as high-risk countries;
c) other cases of high risk identified by the UIFAND or the parties under obligation according to, among others, the following high-risk situation evidences:
   1) Customer risk factors:
      a) the business relationship is conducted in unusual circumstances;
      b) customers that are resident in geographical areas of higher risk as set out in point 3);
      c) legal persons or arrangements that are personal asset-holding vehicles;
      d) companies that have nominee shareholders or shares in bearer form;
      e) cash-intensive businesses;
      f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
      g) customers who are nationals of non European Union Member states and apply for residence rights or citizenship in Andorra in exchange for capital transfers, purchasing property or government bonds, or investing in Andorran corporate entities.
   2) Product, service, transaction or delivery channel risk factors:

a) private banking;
b) products or transactions that might favour anonymity;
c) non-face-to-face business relationships or transactions, without certain safeguards, such as relevant means of eletronic identification in accordance with Law 35/2014, of November 27, on electronic trust services;
d) payments received from unidentified persons or unassociated third parties;
e) new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;
f) transactions related to oil, arms, precious metals, tobacco products, cultural artifacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

3) Factors de risc en funció de l'àrea geogràfica:
a) països d'alt risc en els termes que estableix l'article 6 d'aquesta Llei;
b) països que, segons fonts fiables i independents, tinguin nivells significatius de corrupció o altres activitats delictives;
c) països objecte de sancions, embargaments o mesures similars adoptades per la Unió Europea o per les Nacions Unides;
d) països que ofereixin finançament o suport a activitats terroristes, o en el territori dels quals operin organitzacions terroristes.

Enhanced customer due diligence measures need not be invoked automatically with respect to branches or majorityowned subsidiaries of parties under obligation located in high-risk countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with article 41 of this Law.

The UIFAND may issue guidelines on enhanced customer due diligence measures which are appropriate and proportionate to the nature and size of the parties under obligation.

2. Parties under obligation shall examine, as far as reasonably possible, the background and purpose of all transactions that fulfil at least one of the following conditions:

a) they are complex transactions;
b) they are unusually large transactions;
c) they are conducted in an usual pattern;
d) they do not have an apparent economic or lawful purpose.

In particular, parties under obligation shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

Article 12 bis. High risk countries

1. With respect to business relationships or transactions involving high-risk third countries identified pursuant to the procedure in paragraph 1 of article 6 of this Law, parties under obligation shall:

a) obtain additional information on the customer and on the beneficial owner(s);
b) obtain additional information on the purpose and intended nature of the business relationship;
c) obtain information on the source of funds and source of wealth of the customer and of the beneficial owner(s);
d) obtain information on the reasons for the intended or performed transactions;
e) obtain the approval from senior management for establishing or continuing the business relationship;
f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Article 13. Correspondent banking relationships

1. With respect to cross-border correspondent relationships with entities of other countries, the correspondent Andorran banking and financial entities shall:

a) gather sufficient information about the foreign respondent entity to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the entity and the quality of supervision, including if it has been subject to an investigation or any other regulatory action concerning money laundering or terrorist financing.
b) assess that the respondent entity's money laundering and terrorist financing controls are adequate and effective.
c) obtain approval from senior management before establishing new correspondent banking relationships.
d) document the respective responsibilities of each entity.
e) with respect to payable-through accounts, be satisfied that the foreign respondent entity has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the Andorran correspondent entity, and that it is able to provide the necessary data for the purposes of identification and verification of the customer and of the beneficial owner to the correspondent entity, upon request.

2. Establishing or continuing correspondent banking relationships with shell banks is prohibited. Appropriate measures shall be taken to ensure that no correspondent banking relationships are established or maintained with banks that are known to permit their accounts to be used by shell banks.

Article 14. Policitally exposed persons (PEPs)

In relation to transactions or business relationships with politically exposed persons, parties under obligation shall:

a) have in place appropriate risk management systems to determine whether a customer or the beneficial owner of the customer is a politically exposed person;
b) obtain senior management approval for establishing or continuing a business relationship with politically exposed persons;

c) take adequate measures to establish the source of wealth and source of funds that are involved in business relationship or transactions;
d) conduct enhanced, ongoing monitoring on that relationship.

These obligations are also applicable where, after having initially identified and verified a customer or beneficial owner, such customer or beneficial owner becomes a politically exposed person.

Article 15. Life Insurance with politically exposed persons

Parties under obligation take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons, their family members and persons known to be associates. Those measures shall be taken no later at the time of the payout or at the time of the assignment, in whole or in part, of the policy. Where there are higher risks identified, in addition to applying the customer due diligence measures laid down in article 9 of this Law, parties under obligation shall:

a) inform senior management before payout of policy proceeds;
b) conduct enhanced scrutiny of the entire business relationship with the policyholder;
c) consider the submission of a suspicious transaction report.

Article 16. Termination of enhanced customer due diligence measures in case of PEPs

Where a politically exposed person is no longer entrusted with the public function, for which had this consideration, parties under obligation shall continue applying enhanced customer due diligence measures laid down in article 14 for at least twelve months.

Article 17. Family membres or persons known to be close associates of PEPs

The measures referred to in articles 14 and 15 of this Law shall also apply to family members or persons known to be close associates of politically exposed persons.

Section 4. Performance by third parties

Article 18. Performance by third parties

1. Parties under obligation may rely on third parties to meet the customer due diligence requirements laid down in points a), b), and c) of paragraph 1 of article 9 of this Law. However, the ultimate responsibility for meeting those requirements remains with the party under obligation which relies on the third party.

2. For the purposes of the previous paragraph, 'third parties' means parties under obligation listed in article 2 of this Law, or other entities or persons situated in other countries that:

a) apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this Law; and
b) have their compliance with the requirements of domestic law supervised in a manner consistent with the Andorran legislation.

3. Parties under obligation shall not delegate the performance of the customer due diligence requirements laid down in points a), b), c) of paragraph 1 of article 9 of this Law on third parties established in high-risk countries referred to in article 6.

4. Parties under obligation, without prejudice to remain the ultimate responsible with respect to the customer, may accept the customer due diligence measures performed by their parent companies or branches and majority-owned subsidiaries established in Andorra or in another country which fully comply with the group-wide policies and procedures in accordance with article 41 of this Law.

5. Parties under obligation shall obtain from the third party relied upon the necessary information concerning the customer due diligence requirements laid down in letters a), b) and c) of paragraph 1 of article 9 of this Law.

Likewise, parties under obligation shall take adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification of the identity documents and other relevant documentation on the identity of the customer or the beneficial owner, as well as the documents, information or data on the purpose and intended nature of the business relationship, including, where available, data obtained through relevant electronic identification means as set out in the Law on electronic trust services in force.

6. This regime shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the party under obligation.

Capter III. Beneficial owner information of Andorran legal entities

Article 19. Obligation to obtain, hold and access information on beneficial owners

1. Corporate and other legal entities incorporated in the Principality of Andorra are required to obtain and hold adequate, accurate and current information on their beneficial ownership.

Those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to parties under obligation when the parties under obligation are taking customer due diligence measures in accordance with chapter II of this Law.

The beneficial owners are obliged to provide corporate or other legal entities constituted in the Principality of Andorra with all the information necessary to comply with the requirements in the first paragraph, according to the legislation on Corporations, Associations and Foundations.

2. Information referred to in paragraph 1 can be accessed in a timely manner by the UIFAND and other competent authorities.

3. The Companies Register, the Associations Register and the Foundations Register shall require the information on the beneficial owners of the entities registered in the terms set out by the legislation. The information held is accurate and current.

The parties under obligation and, if appropriate and to the extent that this requirement does not interfere unnecessarily with their functions, competent authorities, shall report to the

Registers any discrepancy that they find between the beneficial owner information recorded in the relevant Register and the information available to them.

In the case of reported discrepancies, the Register shall take appropriate actions to resolve the discrepancies in a timely manner and, if appropriate, include a specific mention in the meantime.

4. Information on beneficial owners held by the Companies Register, the Associations Register and the Foundations Register shall in all cases be accessible to:

a) the UIFAND, tax authorities, Andorran Financial Authority, the Ministry of Finance, the legal authorities, the Public Prosecutor, the Police and any other competent authorities in the field of the prevention and fight against money laundering, related predicate offences and terrorist financing, tracing and seizure or confiscation of criminal assets, without any restriction;
b) parties under obligation, within the framework of customer due diligence measures in accordance with chapter II;
c) any other person not included in the previous letters.

The persons referred to in letter c) shall be permitted to access, at least, the name, surname, month and year of birth, nationality and country of residence of the beneficial owner, as well as the extent of their beneficial ownership status.

Access to information on beneficial ownership kept in the Companies Register, the Associations Register and the Foundations Register shall be in accordance with data protection rules and may be subject to online registration and to the payment of a fee. The fees charged for obtaining the information shall not exceed the administrative costs thereof, including costs of maintenance and development of the register.

5. Parties under obligation do not rely exclusively on the Companies Register, the Associations Register and the Foundations Register to fulfil their customer due diligence requirements in accordance with chapter II.

6. An exemption to the access to all or part of the information on the beneficial owner to the persons referred to in paragraph 4, letters b) and c) is granted, when such access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable. This exemption shall not apply to financial parties under obligation, notaries and saigs.[1]

The procedure to request limits on access to information is developed by regulations. Interested persons may appeal the decision denying the exemption in accordance with the Administrative Code.

Chapter IV. Reporting obligations and prohibition of disclosure.

Article 20. Obligation to report

[1] bailiff, a specialist and independent executor who has the authority to execute judicial decisions under the control of the body that has issued such decisions

1. Parties under obligation are subject to the following obligations:

a) reporting to the UIFAND, on their own initiative, any transaction or attempted transaction related to the funds where the party under obligation is aware of, knows, suspects or has reasonable grounds to suspect that are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests made by the UIFAND for additional information in such cases; and
b) providing the UIFAND, at its request, with all necessary information in the exercise of its functions.

All suspicious transactions, including attempted transactions, shall be reported.

2. Notaries, lawyers and other independent legal professionals and external accountants shall not apply the obligation to report suspicious transactions only to the strict extent that such exemption relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of the client, or performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

3. The obligation to report shall be met regardless of the country where the alleged offence of money laundering or terrorist financing has been committed or could have been committed, or where the funds come from or are destined.

The report shall be made before the party under obligation has carried out the suspicious transaction.

Once the report has been made or after an information request, parties under obligation shall submit to the UIFAND any new element concerning the report they are aware of.

4. The representative of the party under obligation before the UIFAND files the suspicious transaction report referred to in paragraph 1.

5. If, in the light of the investigations carried out in the exercise of its functions, the UIFAND considers that there are sufficient indicia, it may order the provisional suspension of the transaction or transactions as it deems appropriate.

The suspension may not exceed five days, which is the maximum deadline that the UIFAND has to lift it if such indicia have been disproven or, otherwise, it shall submit the file to the Public Prosecutor's Office.

6. Under no circumstances will the UIFAND be liable for any loss or damage suffered as a result of the freezing of assets ordered within the scope of its functions.

Article 21. Obligation to report to self-regulatory bodies and professional bodies

1. By way of derogation from the previous article, the UIFAND, by means of a technical communiqué, may designate a self-regulatory body or professional body of the profession concerned as the authority to which submit the report, instead of the UIFAND. In this case, self-regulatory bodies shall forward the information to the UIFAND promptly and unfiltered.

2. The self-regulatory body or professional bodies shall publish an annual report containing information on:

a) measures taken by the competent authorities in the context of sanction proceedings under articles 69 to 78 of this Law, regarding the members they represent;
b) the number of reports of breaches received as referred to in article 91 of this Law, where applicable;
c) the number of suspicious transactions reports received and the number of reports forwarded to the UIFAND, where applicable;
d) where applicable, the number and description of measures taken to monitor compliance by parties under obligation with their obligations under:
    i) articles 7 to 17 (customer due diligence);
    ii) articles 20, 21 and 22 (suspicious transaction reporting);
    iii) article 37 (record keeping);
    iv) articles 40, 41 and 42 (internal procedures and training).

Article 22. Refraining from carrying out transactions

1. Parties under obligation shall refrain from carrying out transactions which they know or suspect or their reasonable grounds to be related to proceeds of criminal activity or terrorist financing until they have completed the report to the UIFAND and have complied with any further specific instruction from it.

2. When refraining from carrying out suspicious economic or financial transactions is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected operation, parties under obligation may carry out the transaction and inform the UIFAND immediately afterwards. The report shall include, in addition to the information laid down in article 20 of this Law, the reasons which have justified carrying out the transaction.

Article 23. Obligation to report by the supervisory bodies

If, in the course of checks carried out on the parties under obligation by the competent authorities for prudential supervision, or in any other way, those authorities discover facts that could be related to money laundering or to terrorist financing, they shall promptly inform the UIFAND.

Article 24. Effects of the reporting made by parties under obligation

Disclosure information in good faith to the UIFAND by a party under obligation or its employees or directors shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the parties under obligation or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether illegal activity actually occurred.

Article 25. Protection of parties under obligation

1. The UIFAND and any other administrative or judicial authority shall take all appropriate measures to protect the parties under obligation against any threat, retaliatory or hostile action arising from complying with the obligations imposed by this Law and in particular from adverse

or discriminatory employment actions. In particular, the identity of the party under obligation and of the employees who have taken part in the suspicious transaction reports and in all administrative and legal proceedings originating from or related to the reports made, will be kept confidential.

2. To this purpose, the UIFAND assesses the suspicious transaction report and, in the event of finding indicia or the existence of money laundering or terrorist financing, it reports to the Public Prosecutor's Office. The UIFAND's report does not incorporate or make reference to the suspicious transaction reports of the parties under obligation, its employees or directors nor to their identification or to that of the civil servants or members of the UIFAND intervening in the instruction.

3. The UIFAND report has the probative value considered by the judicial authorities and it may be incorporated to the arising judicial or administrative proceedings deriving therefrom.

Information classified as financial intelligence by the UIFAND cannot be incorporated to the judicial or administrative proceedings.

4. Except in the event of criminal prejudiciality, if the UIFAND observes, in the exercise of its functions, irregularities which are the competence of another administrative body, it shall send the respective report to such other body, maintaining confidentiality with respect to the identity of the party under obligation and of the employees intervening in the declarations of suspicion and in all the administrative and legal proceedings originating from or related to the declarations made.

5. Individuals who are exposed to threats, retaliatory or hostile actions, or adverse or discriminatory employment actions for reporting suspicions of money laundering or terrorist financing internally or to the UIFAND, are entitled to file a complaint before the UIFAND, which shall analyse it and, in the event it finds evidence of or verifies the existence of a criminal offence, report to the Public Prosecutor.

Article 26. Prohibition of disclosure

1. Parties under obligation and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted to the UIFAND or that a money laundering or terrorist financing analysis is being, or may be, carried out.

2. With regard to suspicious transaction reports, this prohibition of disclosure shall not include disclosure to the competent authorities, including the self-regulatory bodies, provided that such disclosure is authorised in writing by the UIFAND.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between financial parties under obligation and their branches and majority-owned subsidiaries located in other countries, provided that those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with article 41 of this Law, including procedures for sharing information within the group, and that the group-wide policies and procedures comply with the requirements laid down in this Law, provided that this disclosure is authorised in writing by the UIFAND.

4. The prohibition laid down in paragraph 1 shall not prevent disclosure of information relating suspicious transaction reports, provided that the UIFAND so authorises in writing, between the parties under obligation as referred to in points a) and b) of paragraph 2 of article 2, or entities from other countries which impose requirements equivalent to those laid down in this Law, who perform their professional activities, whether as employees or not, within the same legal person or a larger structure to which the person belongs and which shares common ownership, management or compliance control.

5. The prohibition laid down in paragraph 1 shall not prevent disclosure of information relating suspicious transaction reports, provided that the UIFAND so authorises in writing, in cases relating to the same customer and the same transaction involving two or more parties under obligation, whether financial or not financial referred to in points a) and b) of paragraph 2 of article 2, provided that they are from the same professional category and are subject to obligations as regards professional secrecy and personal data protection. Information exchanged is used exclusively for the purposes of preventing money laundering and terrorist financing.

6. Where the parties under obligation referred to in points a) and b) of paragraph 2 of article 2 seek to dissuade a client from engaging in illegal activity, that shall not constitute disclosure within the meaning of paragraph 1 of this article.

Chapter V. Information on the payer acccompanying wire transfers

Section 1. Subject-matter, scope and definitions

Article 27. Subject-matter

This section lays down rules on the information accompanying wire transfers, in any currency, as regards the payers and beneficiaries thereof, where at least one of the payment service provider involved in the transfer is established in Andorra.

Article 28. Scope

1. This chapter applies to wire transfers, in any currency, which are sent or received by a payment service provider or intermediary payment service provider established in Andorra.

2. This chapter does not apply to the services listed in letters a) to m) and o) of section 3 of article 2 of the Law on payment services and electronic money.

3. This chapter does not apply to wire transfers carried out using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, provided that:

a) that card, instrument or device is used exclusively to pay for goods or services; and
b) the number of that card, instrument or device accompanies all transfers flowing from the transaction.

However, this chapter applies when a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, is used in order to effect a person-to-person transfer of fund.

4. This chapter does not apply to persons that have no activity other than to convert paper documents into electronic data and that do so pursuant to a contract with a payment service provider, or to persons that have no activity other than to provide payment service providers with messaging or other support systems for transmitting funds or with clearing and settlement systems.

This chapter does not apply to wire transfers:

a) that involve the payer withdrawing cash from the payer's own payment account;
b) that transfer funds to a public authority as payment for taxes, fines or other levies within Andorra;
c) where both the payer and the payee are payment service providers acting on their own behalf;
d) that are carried out through cheque images exchanges, including truncated cheques.

5. This chapter does not apply to wire transfers within Andorra to a payee's payment account permitting payment exclusively for the provision of goods or services where all of the following conditions are met:

a) the payment service provider of the payee is subject to this Law;
b) the payment service provider of the payee is able to trace back, through the payee, by means of a unique transaction identifier, the wire transfer from the person who has an agreement with the payee for the provision of goods or service;
c) the amount of the wire transfer does not exceed EUR 1,000.

Article 29. Definitions

For the purposes of this chapter, the following definitions apply:

1. **Payer**: means a person that holds a payment account and allows a wire transfer from that payment account, or, where there is no payment account, that gives a wire transfer order.

2. **Payee**: means a person that is the intended recipient of the wire transfer.

3. **Payment service provider**: means the entities listed in section 1 of article 4 of the Law on payment services and electronic Money.

4. **Intermediary payment service provider**: means every payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a wire transfer on behalf of the payment service provider of the payer or of the payee or of another intermediary payment service provider.

5. **Payment account**: means a payment account as defined in section 8 of article 3 of the Law on payment services and electronic money.

6. **Funds**: means the definition of section 22 of article 3 of the Law on payment services and electronic money.

7. **Wire transfer**: means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to

a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:

a) credit transfers, as defined in section 45 of article 3 of the Law on payment services and electronic money;
b) direct debits, as defined in section 17 of article 3 of the Law on payment services and electronic money;
c) money remittance, as defined in section 39 of article 3 of the Law on payment services and electronic money;
d) transfers carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.

8. **Batch file transfer**: means a bundle of several individual wire transfers put together for transmission.

9. **Unique identifier:** means a combination of letters, numbers or symbols determined by the payment service provider that the user of those services must provide in order to unambiguously identify another user of payment services and/or a payment account in a payment operation.

10. **Person-to-person wire transfer**: means a transaction between natural persons acting, as consumers, for purposes other than trade, business or profession.

Section 2. Obligations on the payment service provider of the payer

Article 30. Information accompanying wire transfers

1. The payment service provider of the payer shall ensure that wire transfers are accompanied by the following information on the payer:

a) the name of the payer;
b) the payer's payment account number; and
c) the payer's address, official personal document number, customer identification number or date and place of birth.

2. The payment service provider of the payer shall ensure that the transfer funds are accompanied by the following information on the payee:

a) the name of the payee, and
b) the payee's payment account number.

3. By way of derogation from point b) of paragraph 1 and point b) of paragraph 2, in the case of a transfer not made from or to a payment account, the payment service provider of the payer shall ensure that the wire transfer is accompanied by a unique transaction identifier rather than the payment account number(s).

4. Before transferring funds, the payment service provider of the payer shall verify the accuracy of the information referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source.

5. Verification as referred to in paragraph 4 shall be deemed to have taken place where:

a) a payer's identity has been verified in accordance with article 9 of this Law and the information obtained pursuant to that verification has been stored in accordance with article 37 of this Law; or
b) the payee falls within the scope of paragraph 5 of article 10 of this Law.

6. The payment service provider of the payer shall not execute any wire transfer before ensuring full compliance with this article.

7. The provisions of this article also apply to batch transfers.

Section 3. Obligations on the païment service provider of the payee

Article 31. Detection of missing information on the payer or the payee

1. The payment service provider of the payee shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to execute the wire transfer have been filled in using characters or inputs admissible in accordance with the conventions of that system.

2. This payment service provider shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the information referred to in paragraphs 1 and 2 of article 30 is missing. These procedures also apply to batch file transfers.

3. In the case of wire transfers exceeding EUR 1,000, whether those transfers are carried out in a single transfer or in several transfers which appear to be linked, before crediting the payee's payment account or making the funds available to the payee, the payment service provider of the payee shall verify the accuracy of the information on the payee referred to in paragraph 2 of this article on the basis of documents, data or information obtained from a reliable and independent source, without prejudice of the requirements provided by article 23 of the Law on payment services and electronic money and its Regulations.

4. In the case of wire transfers not exceeding EUR 1,000 that do not appear to be linked to other wire transfers which, together with the transfer in question, exceed EUR 1,000, the payment service provider of the payee need not verify the accuracy of the information on the payee, unless the payment service provider of the payee:

a) effects the pay-out of the funds in cash or in anonymous electronic money; or
b) has reasonable grounds for suspecting money laundering or terrorist financing.

5. Verification as referred to in paragraphs 3 and 4 shall be deemed to have taken place where:

a) a payee's identity has been verified in accordance with article 9 of this Law and the information obtained pursuant to that verification has been stored in accordance with article 37 of this Law; or
b) the payer falls within the scope of paragraph 5 of article 10 of this Law.

Article 32. Wire transfers with missing or incomplete information

1. The payment service provider of the payee shall implement effective risk-based procedures, including the risk analysis procedure referred to in article 9 of this Law, for determining whether to execute, reject or suspend a wire transfer lacking the required complete payer and payee information and for taking the appropriate follow-up action.

Where the payment service provider of the payee becomes aware, when receiving wire transfers, that the information referred to in paragraphs 1 and 2 of article 30 is missing or incomplete or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in paragraph 1 of article 31, the payment service provider of the payee shall reject the transfer or ask for the required information on the payer and the payee before or after crediting the payee's payment account or making the funds available to the payee, on a risk-sensitive basis.

2. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future wire transfers from that payment service provider, or restricting or terminating its business relationship with that payment service provider.

The payment service provider of the payee shall report to the UIFAND that failure, and the steps taken.

Article 33. Assessment and reporting of suspicious transactions

The payment service provider of the payee shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a wire transfer, or any related transaction, is suspicious and whether it is to be reported to the UIFAND.

Section 4. Obligations on intermediary paymenet service providers

Article 34. Retention of information on the payer and the payee with the transfer

Intermediary payment service providers shall ensure that all information received on the payer and the payee that accompanies a wire transfer is retained with the transfer.

Article 35. Detection of missing information on the payer or payee

1. The intermediary payment service provider shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the wire transfer have been filled in using characters or inputs admissible in accordance with the conventions of that system.

2. The intermediary payment service provider shall implement effective procedures, including, where appropriate, expost monitoring or real-time monitoring, in order to detect whether the information on the payer and the payee referred to in paragraphs 1 and 2 of article 30 is missing. These procedures also apply to batch file transfers.

Article 36. Wire transfers with missing ingormation on the payer or the payee

1. The intermediary payment service provider shall establish effective risk-based procedures for determining whether to execute, reject or suspend a wire transfer lacking the required payer and payee information and for taking the appropriate follow up action.

Where the intermediary payment service provider becomes aware, when receiving wire transfers, that the information referred to in paragraphs 1 and 2 of article 30 of this Law is missing or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in paragraph 1 of article 31 of this Law shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the wire transfer, on a risk-sensitive basis.

2. Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the intermediary payment service provider shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future wire transfers from that payment service provider, or restricting or terminating its business relationship with that payment service provider.

The intermediary payment service provider shall report to the UIFAND that failure, and the steps taken..

3. The intermediary payment service provider shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a wire transfer, or any related transaction, is suspicious and whether it is to be reported to the UIFAND.

Chapter VI. Record-retention and data protection

Article 37. Record retention

1. . Parties under obligation shall retain, for five years, all documents, data and information obtained under the application of this Law, receipts and registers of operations and transactions, account files and business correspondence, and the results of any analysis undertaken, including, where available, information obtained through electronic identification means as set out in the Law on electronic trust services.

This period of record keeping starts from the date of termination of the business relationship or the date of the occasional transaction.

These documents shall include information on the identity of the customer, the nature and date of the transaction, the source of funds, the currency, the amount of the transaction, and the purpose and intended nature of the business relationship with the customer.

2. The UIFAND may further extend the retention period referred to in the paragraph 1 of this article for a maximum period of five years, in an individual and reasoned manner.

3. Parties under obligation shall ensure that the information referred to in paragraph 1 is made available to the competent authorities as soon as it is required.

4. Parties under obligation shall act diligently to verify the documents, information and any other data required to their customers to comply with this Law.

5. Financial parties under obligation shall electronically store the copies of the data and information on the customer and its beneficial owner obtained under this Law and its developing provisions. In any case, the filing system of the parties under obligation shall ensure the appropriate management and availability of the documentation for internal control purposes as well as to meet in a timely and appropriate manner the requests made by the competent authorities.

6. The information referred to in paragraph 1 shall be sufficient to permit reconstruction of individual transactions in the case of investigations carried out by the UIFAND or other competent authorities.

Article 38. Data protection

1. Personal data shall be processed by the parties under obligation on the basis of this Law only for its purposes and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Law for any other purposes, such as commercial purposes, is prohibited.

2. Parties under obligation provide new clients with the general information on the legal obligations of the parties under obligation for the purposes of the prevention of money laundering and terrorist financing.

3. Processing of personal data obtained under this Law is not subject to the provisions on personal data protection.

Article 39. Responses to information requests

Parties under obligation have systems in place that enable them to respond fully and speedily to enquiries from the UIFAND and other competent authorities in the exercise of their functions, through secure channels and in a manner that ensures full confidentiality of the enquiries.

Chapter VII. Internal procedures and training

Article 40. Internal procedures

1. Financial parties under obligation shall:

a) contract an independent external audit to verify compliance with this Law and send a copy of the report issued for this purpose to the UIFAND;
b) appoint an internal control and communication body in charge of organising and monitoring compliance with the rules on prevention against money laundering and terrorist financing and notify this appointment to the UIFAND;
c) establish internal audit and control procedures aimed at verifying compliance with regulations, detecting, preventing and effectively managing the money laundering and terrorist financing risks.

The UIFAND may establish, by means of a technical communiqué, the criteria to be followed in audits.

2. Parties under obligation which are legal entities shal:

a) appoint an internal control and communication body in charge of organising and monitoring compliance with the provisions on the prevention of money laundering and terrorist financing and notify this appointment to the UIFAND.
The members of the internal control and communication body shall be members of the management or the senior management of the party under obligation.
b) establish the internal control procedures.

3. Non-financial parties under obligation which are natural persons that conduct activities which determine their status as parties under obligation, will be considered to be their own internal control and communication body.

4. Parties under obligation shall designate, at least, one manager who is a member of the internal control and communication body, as a representative before the UIFAND, on the basis of the person's training, suitability and experience in the sector.

5. The representatives before the UIFAND of the parties under obligation have, in all cases, the following functions:

a) to submit the suspicious transaction reports referred to in Article 20 of this Law;
b) to receive the inquiries and requests from the UIFAND..

6. Where a natural person falling within any of the categories listed in Article 2, Paragraph 2 of this Law performs professional activities as an employee of a legal entity, the obligations of this section shall apply to that legal entity rather than to the natural person.

7. Financial parties under obligation which carry out financial activities occasionally or in a very limited way may be exempted by regulatory means from compliance with any or all of the provisions established in this article, when there is a low risk of money laundering or terrorist financing.

Article 41. Internal controls in parties under obligation that are part of a group

1. 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 money laundering and terrorist financing purposes. Those policies and procedures shall be implemented effectively at the level of branches and majority-owned subsidiaries in other countries.

2. Parties under obligation that operate branches in other countries shall ensure that those branches respect the national provisions on prevention of money laundering and terrorist financing.

3. Where parties under obligation have branches or majority-owned subsidiaries located in countries where the minimum requirements on prevention of money laundering and terrorist financing are less strict than those of Andorra, their branches and majority-owned subsidiaries located in other countries shall implement the requirements of Andorra, to the extent that the law of the country in which are located the branches or majority-owned subsidiaries, so allows.

4. Parties under obligation, where the law of the other country does not permit the implementation of the policies and procedures required under paragraph 1, shall ensure that

branches and majority-owned subsidiaries in that country apply additional measures to effectively handle the risk of money laundering or terrorist financing, and inform the UIFAND. If the additional measures are not sufficient, the UIFAND shall exercise additional supervisory actions, including requiring that the group does not establish or that it terminates business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the country concerned. The UIFAND shall inform the Andorran Financial Authorty when any of the circumstances included in this paragraph occurs.

The additional measures to be adopted by the parties under obligation referred to in this paragraph, including minimum measures, shall be developed by regulations. These regulatory measures, without prejudice of the measures that the UIFAND may require, may include:

a) that the branch or majority-owned subsidiary terminates the business relationship that, where appropiate, creates the risk;
b) that the branch or majority-owned subsidiary does not carry out the occasional transaction that, where appropiate, creates the risk;
c) closing down some or all of the operations provided by their branch and majority-owned subsidiary established in the other country.

5. Unless the UIFAND states otherwise, the information on suspicious transactions shall be shared within the group, for the purposes of having an aggregated view of the entities' risks, that allows to detect funds which may be the proceeds of criminal activity or may be related to terrorist financing.

Article 42. Training

1. Parties under obligation shall take measures proportionate to their risks, nature and size so that their employees are aware of the provisions on the prevention and fight against money laundering and terrorist financing.

Those measures shall include participation of their employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

2. The UIFAND, by means of training programs or technical communiqués, informs parties under obligation on the practices of money launderers and financers of terrorism and on indications leading to the recognition of suspicious transactions.

3. The UIFAND provides to the parties under obligation, where practicable, timely feedback on the effectiveness of and follow-up to their suspicious transaction reports.

Chapter VIII. Declaration of cross-border transportation of cash

Article 43. Obligation to declare

1. Any natural person entering or leaving the Principality of Andorra and carrying cash of a value of EUR 10,000 or more or its equivalent in foreign currency shall declare that sum to the Customs in accordance with this chapter. The obligation to declare shall not have been fulfilled if the information provided is incorrect or incomplete.

2. The declaration referred to in paragraph 1 shall contain details of:

a) the declarant, including full name, date and place of birth and nationality;
b) the owner of the cash;
c) the intended recipient of the cash;
d) the amount and nature of the cash;
e) the origin and intended use of the cash;
f) the transport route;
g) the means of transport.

3. Information shall be provided either in writing or electronically under the terms set forth in the regulations, and according to the model declaration attached in the regulations. Where a written declaration has been lodged, an endorsed copy shall be delivered to the declarant.

Article 44. Control and inspection powers

1. In order to check compliance with the obligation to declare laid down in the previous article, Customs officials are empowered to carry out controls on natural persons, their baggage and their means of transport.

2. A failure to declare, where this is required, or the lack of veracity in the reported data, shall lead to the seizure by the Customs officials of all the cash carried and/or discovered, with the possibility of an exception of EUR 1,000 in concept of mínimum survival amount.

3. Where, regardless the obligation to declare, there are suspicions that the cash is related to money laundering or terrorist financing, the Customs officials shall seize all the cash carried and/or discovered, and shall immediately communicate it to the UIFAND and the Police.

The possibility of EUR 1,000 exception in concept of minimum survival amount shall be granted on the basis of the circumstances of the case, such as the persons' need to continue the trip or the lack of any other means of survival.

4. Cash shall be seized for a minimum period of six months, extendable for another six months. Cash seized guarantees the payment of any possible penalties resulting from the infringement proceedings.

5. In the cases of seizure of cash laid down in paragraph 2 of this article, Customs shall deliver the record of the seizure, expressly indicating the circumstances that motivated the seizure.

The record of the seizure shall have probative value, notwithstanding the evidence that could be brought forward by the interested parties in defence of their rights or interests.

Article 45. Recording and processing of information

Customs shall record and process the information obtained from the declaration and the exercise of inspection competences laid down in the previous articles and for statistical purposes provide it to the UIFAND and the Police.

Article 46. Exchange of information

1. The UIFAND and the other competent authorities may provide the equivalent foreign bodies with the information obtained pursuant to the previous articles, under the provisions on international cooperation.

2. Where the cash is related to the proceeds of fraud or any other illegal activity negatively affecting the financial interests of the European Union, this information shall also be provided to the European Commission.

Article 47. Penalties

1. Breach of the obligation to declare referred to in article 43 of this Law shall be deemed as a serious infringement and shall be punished with a minimum fine of EUR 600 up to the amount of the cash carried.

2. The power to punish the breach of the obligation to declare, as laid down in article 43 of this Law, lies with Customs. The infringement proceedings are governed in accordance with those applicable to customs.

3. The criteria laid down in article 77 of this Law shall be taken into account for the purposes of determining the penalty imposed.

Chapter IX. Measures for the prevention, fight and suppression of terrorisme and its financing and the prevention and disruption of the proliferation of weapons of mass destruction and its financing

Sole section. List of persons and entities and restrictive measures

Article 48. List of persons and entities

1. The Permanent Committee for the prevention and fight against money laundering and terrorist financing shall prepare and release for public knowledge on the UIFAND website a list of the names and circumstances of persons and entities deemed to have links with terrorist activities, its financing, or the financing of the proliferation of weapons of mass destruction.

The Permanent Committee for the prevention and fight against money laundering and terrorist financing obtains, through its members, all possible information to identify and determine the identity and the circumstances of persons and entities that, based on reasonable grounds, are deemed to meet the criteria for inclusion on the list or may reasonably be suspected to or be believed to meet these criteria.

There shall be reasonable grounds to include on the list the persons or entities linked with the aforementioned activities and they shall be so included by a specific resolution of the Permanent Committee for the prevention and fight against money laundering and terrorist financing stating that there is reasonable evidence that they are terrorists, finance terrorism, finance the proliferation of weapons of mass destruction, or belong to organisations involved in the same.

The existence of criminal proceedings against a person or entity is not a necessary requirement for inclusion in the list, although it does constitute reasonable grounds for inclusion.

2. In any case, the list shall include the names and circumstances of persons and entities listed by the corresponding United Nations committee.

3. If a state so requests, the Permanent Committee for the prevention and fight against money laundering and terrorist financing may decide to include a person or entity on the list if it considers that there are reasonable grounds or a reasonable basis to suspect that the person or entity whose inclusion is requested is involved in terrorism, terrorist financing, financing the proliferation of weapons of mass destruction, or belongs to organisations involved in the same.

4. The Permanent Committee for the prevention and fight against money laundering and terrorist financing may include and/or remove persons and entities from the list based on the merits of the information received and, where necessary, taking into account the criteria and procedures set forth in the United Nations resolutions.

5. The Permanent Committee for the prevention and fight against money laundering and terrorist financing may propose persons or entities to be included in the respective list of other states and competent United Nations committees if the persons and entities submitted meet the specific criteria for inclusion in the lists in accordance with resolutions of the United Nations Security Counci.

Article 49. Restrictive measures

1. The Permanent Committee for the prevention and fight against money laundering and terrorist financing shall agree to and publish, without delay, the restrictive measures adopted, where appropriate, following the resolutions of the United Nations Security Council or any of its committees.

2. The restrictive measures may include:

a) freezing all funds and economic resources owned, in possession or directly or indirectly controlled, by the persons or entities referred to in paragraph 3, whether these funds and assets are owned/controlled in full or in conjunction with others, and including funds derived from or having their origin in the above;
b) banning the persons and entities referred to in paragraph 3 below from directly or indirectly accessing any funds, economic resources, financial services, or other related services;
c) placing restrictions on commercial activity, including restrictions on imports and exports and arms embargoes;
d) placing restrictions on financial activities of any nature, including assessment, support, and procurement services;
e) any other restriction, including technical assistance, flight bans and restrictions on admission and transit;
f) diplomatic sanctions, the suspension of cooperation, and boycotting sports events in case of countries included in the lists adopted by the relevant committee of the United Nations.

3. The restrictive measures apply to:

a) persons and entities included on the list;

b) any entity that is either owned or directly or indirectly controlled by any person or entity on the list;
c) any person or entity acting on behalf or under the instructions of a person or entity on the list;
d) countries included in the lists adopted by the corresponding committee of the United Nations in relation to diplomatic sanctions, suspensions of cooperation and boycott of sport events.

4. The Permanent Committee for the prevention and fight against money laundering and terrorist financing may adopt restrictive measures or other specific guidelines, in line with recommendations made in resolutions drawn up by the United Nations Security Council or any of its committees.

5. While adopting restrictive measures, the Permanent Committee for the prevention and fight against money laundering and terrorist financing may also agree to derogations or limitations following the resolutions drawn up by the United Nations Security Council or one of its committees for reasons of public order or in the public interest.

6. The Permanent Committee for the prevention and fight against money laundering and terrorist financing shall proceed with the modifications and derogations included in the restrictive measures, in accordance with resolutions drawn up by the United Nations Security Council or any of its committees.

Article 50. Publication of the list and restrictive measures adopted

1. The list of persons or entities affected and restrictive measures adopted by the Permanent Committee for the prevention and fight against money laundering and terrorist financing shall be published on the website of the UIFAND for the availability of the general public.

2. The Permanent Committee for the prevention and fight against money laundering and terrorist financing shall also publish the following resolutions:

a) the removal of persons or entities from the list;
b) whenever funds or other economic resources owned by persons or entities on the list are again made available;
c) whenever funds or other economic resources owned by persons or entities that had been unduly affected by the freeze decision are again made available, after verifying that these persons or entity are not those designated on the list;
d) the removal of any restrictive measure that was previously adopted.

3. The publication on the UIFAND website will consist of the resolution adopting the measures mentioned above, in addition to the list received from the United Nations Security Council or one of its committees and/or the list of persons or entities that the Permanent Committee for the prevention and fight against money laundering and terrorist financing has taken measures against.

4. Notwithstanding the publication on the UIFAND website, the Permanent Committee for the prevention and fight against money laundering and terrorist financing provides parties under obligation with the names of persons or entities on the list and clear instructions with the

specific measures that shall be taken, whether by email or by any other means that provides proof of receipt. This notificat.

Article 51. Content and effects of the restrictive measures

1. Freezing assets means a ban on any move, transfer, alteration, use, or dealing with funds in any way that would result a change in their volume, amount, location, ownership, possession, character or destination of these fund or any other change that would enable to use funds including portfolio management, possessed, controlled, directly or indirectly, in the moment of the freezing by the person or entity concerned.

All funds and economic resources will continue to be managed:

a) by the financial entity or other organisation appointed for such purpose by the person or entity that owned or controlled the assets, whether directly or indirectly, before the ban;
b) by any new institution or organisation appointed by the person or entity that owned or controlled the assets, whether directly or indirectly, under the authorisation of the Permanent Committee for the prevention and fight against money laundering and terrorist financing.

Administrative measures are measures considered necessary to cover taxes, fees, compulsory insurance premiums, and bank account maintenance charges, any expenses necessary to maintain and administer the frozen assets, and any other justifiable extraordinary expense.

2. Aside from the provisions of article 54 of this Law, it is prohibited to make any funds or economic resources, financial services or other related services, or the profits derived from the same, available, directly or indirectly, to the persons or entities referred to in paragraph 3 of article 49.

3. Restrictive measures shall be immediately implemented as from their publication on the UIFAND website.

4. Restrictive measures are subsidiary in nature, and may not run in counter to the effect of any other applicable asset freeze or confiscation adopted within a legal proceeding affecting the same funds and economic resources.

5. Without prejudice to the corresponding rights of bona fide third parties, any action that contravene the restrictive measures duly published on the UIFAND website is considered null and void and without effect.

6. In terms of efforts to prevent and disrupt financing of the proliferation of weapons of mass destruction, interest and other payments due are allowed to enter the frozen accounts, including amounts due for contracts, agreements or obligations established before the account was frozen, and without the account needing to be unblocked. Otherwise, freezes do not prevent the person or entity concerned from making any payment or meeting any obligation that arises from a contract signed before the party was included on the list, as long as:

a) it is certain that the contract does not relate to any article, material, equipment, asset, technology, support, training, financial assistance, investment brokerage services, or other services banned by the applicable Security Council resolution;
b) hi it is certain that the payment will not be directly or indirectly received by a person or entity included on the list.

Article 52. Reporting obligations

1. The administrative services that manage public records with information relating to persons or entities on the list shall immediately inform the UIFAND, who will then inform the Permanent Committee for the prevention and fight against money laundering and terrorist financing.

2. Parties under obligation that are related to or have knowledge of the funds or economic resources affected by a restrictive measure shall inform the UIFAND via reliable means of the measures taken in accordance with this Law, as well as any other operation that the person or entity intends to carry out.

This notice shall be given no later than five days after the publication of the resolution adopting the measures by the Permanent Committee for the prevention and fight against money laundering and terrorist financing or after the date the funds or economic resources come into the possession of the person giving notice, should this be the later date.

3. The above notification provided by the administrative services and parties under obligation shall contain information about the parties involved, the amount and nature of the funds or economic resources, transactions, business relationships, and any other information relating to the persons and entities on the list.

4. The Permanent Committee for the prevention and fight against money laundering and terrorist financing, once it has received information about the effectiveness of the freeze or any other restrictive measure, shall:

a) ratify the freeze or impose any other restrictive measure by express communication to the organisation holding the funds or economic resources. The absence of a communication to the fund holder within fifteen days of receipt of the information by the latter will entail confirmation of the measure.
   Once the Permanent Committee for the prevention and fight against money laundering and terrorist financing has adopted the relevant agreement, this correspondence will be notified to the organisation holding the funds or economic resources by means of the UIFAND;
b) notify the parties affected, either directly (if their address is known) or via the publication of a notice in the Official Gazette of the Principality of Andorra. This notice shall contain the following information:
   i) the existence of a freeze or restrictive measure;
   ii) the reasons for the same;
   iii) the content of the same;
   iv) the actions and appeals available in order to totally or partially lift the freeze or the restrictive measure, and to remove names from the list.

Once the Permanent Committee for the prevention and fight against money laundering and terrorist financing has adopted the applicable resolution the person concerned will be notified.

5. The organisation that manages the frozen funds or economic resources shall inform the UIFAND immediately should any problem occur regarding the funds or financial resources. In general, the UIFAND shall be informed of their general status and situation every six months.

6. In any case, the Permanent Committee for the prevention and fight against money laundering and terrorist financing, the UIFAND, and the parties under obligation are not responsible for any damage caused by implementing the restrictive measures and the other provisions included in this chapter.

Article 53. Removal from the list

1. The Permanent Committee for the prevention and fight against money laundering and terrorist financing shall evaluate and resolve in a reasoned manner the requests for removal from the list made by the concerned parties within fifteen days.

2. If approval is given for a person or entity to be removed from the list, the Permanent Committee for the prevention and fight against money laundering and terrorist financing will take the appropriate actions and notify the administrative services and parties under obligation in order to release the funds and economic resources affected by the measures, via the UIFAND.

When registration on the list arises due to a resolution drawn up by the United Nations Security Council or one of its committees, the Permanent Committee for the prevention and fight against money laundering and terrorist financing is not eligible to hear the case and the applicant will be informed of the appeals available to them in order to be removed from the list of the Committee concerned. These appeals include in particular:

a) the option to do this directly in accordance with established procedures, of which the applicant shall be informed; or
b) the option to do so indirectly via the Permanent Committee for the prevention and fight against money laundering and terrorist financing, which shall then address the United Nations Security Council or one of its committees and notify them of the request to be removed from the list.

3. The resolutions of the Permanent Committee for the prevention and fight against money laundering and terrorist financing are administrative in nature. Once the period of fifteen days referred to in paragraph 1 of this article has elapsed, the request for removal from the list shall be understood as having been rejected, allowing the applicant to appeal the decision before the Government.

Article 54. Lifting and modifrying restrictive measures

1. The Permanent Committee for the prevention and fight against money laundering and terrorist financing shall evaluate and hand down a decision within fifteen days in relation to the following:

a) requests made by the parties concerned to lift or modify the action taken; and

b) requests from bona fide third parties affected by the actions taken, either because they bear an identity or similarity to the person or entity concerned in terms of their name or otherwise, or for any other reason that constitutes grounds to lift or modify the measures.

2. If the adopted measures are lifted, whether in full or in part, or if they are modified, the Permanent Committee for the prevention and fight against money laundering and terrorist financing will carry out the necessary procedures to release the funds and economic resources affected and notify the administrative services and the parties under obligation via the UIFAND.

3. The Permanent Committee for the prevention and fight against money laundering and terrorist financing may authorise, upon request, all or part of the frozen funds and economic resources to be used by the persons or entities listed or by family members in order to meet their basic needs, including the cost of food, medication, housing, health care, and legal assistance. The Permanent Committee for the prevention and fight against money laundering and terrorist financing may also authorise the use of frozen funds and financial assets to cover the cost of taxes, fees, compulsory insurance premiums and bank account maintenance charges, as well as any expenses necessary to maintain and administer the frozen assets and any other justifiable extraordinary expense.

4. When the adopted measures arise from compliance with a resolution drawn up by the United Nations Security Council or one of its committees, the Permanent Committee for the prevention and fight against money laundering and terrorist financing may not lift or modify the action taken without proceeded to the respective communications and formalities which are required on a prior basis according to the applicable resolutions.

5. The resolutions of the Permanent Committee for the prevention and fight against money laundering and terrorist financing are administrative in nature and can be appealed before the Government. Once the period of fifteen days referred to in paragraph 1 of this article has lapsed, the request for removal from the list shall be understood as having been rejected, allowing the applicant to appeal the decision.

Chapter X. Institutional organisation

Section 1. UIFAND

Article 55. Powers and functions of the UIFAND

1. The UIFAND is the competent body for launching and coordinating the measures for the detection, prevention of and the fight against money laundering, terrorist financing and the proliferation of weapons of mass destruction.

Its budget is funded under the budget of the State.

2. The UIFAND exercises the following functions:

a) directs and promotes the activities for the detection, prevention of and fight against the use of the entities of the financial system of the country or those of some other nature for money laundering, terrorist financing or the proliferation of weapons of mass destruction. To this effect, the UIFAND may issue technical communiqués, which are

made available to the general public through its website, in order to develop this Law and the regulations developing it, which are of compulsory compliance, and the recommendations and guidelines which it deems appropriate. Likewise, the UIFAND provides to parties under obligation with appropriate information about the formalities required to submit a suspicious transaction report in the terms established in this Law. In this regard, the UIFAND shall approve a model report and guidelines about its use;

b) requests any information or documents from the parties under obligation in the exercise of its functions, and it verifies compliance with this Law and the regulations developing it;
c) carries out on-site inspections to verify compliance with this Law and the regulations developing it and, in particular, analyses the specific dossiers and files which UIFAND may determine;
d) requests from and sends to the judicial authorities, the Department of Police, the Customs Service or any other body of the Administration, any information that is essential for the exercise of its functions;
e) gathers, assembles and analyses the reports of the parties under obligation, and all the written or oral communications received, and it makes an assessment of the fact;
f) conducts operational analysis which focuses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use of the information after dissemination;
g) conducts strategic analysis addressing money laundering and terrorist financing trends and patterns;
h) orders the suspension of the transactions which it deems appropriate when it considers that, in the light of the investigations carried out in the exercise of its functions, there are indicia of an act of money laundering or of terrorist financing;
i) cooperates with other equivalent foreign bodies;
j) sanctions the minor administrative infringements established by this Law;
k) sends to the Government the instructed dossiers in which facts appear that may constitute a serious or very serious administrative infringement, accompanied by a proposal of sanction;
l) sends and receives any information to or from the Andorran Financial Authority and other bodies of the Administration, within the framework of a relationship of mutual cooperation, which is essential for the exercise of its functions;
m) submits to the Public Prosecutor's Office the cases in which reasonable suspicions of the commission of a criminal infringement appear;
n) shelves the remaining cases and keeps the dossiers for at least ten years;
o) submits to the Government legislative or regulatory proposals related to the detection, prevention of and fight against money laundering, terrorist financing and the proliferation of weapons of mass destruction, and gives advice to the Government in these matters;
p) prepares and publishes annual reports and statistics to assess the effectiveness of the prevention of and fight against money laundering, the financing of terrorist and the proliferation of weapons of mass destruction;
q) designates the self-regulating body or the professional association of the activity concerned as the body to which the non-financial parties under obligation shall report in first instance;
r) exercises any other function that may be assigned to it by Law.

3. The UIFAND, in the exercise of its supervisory functions:

a) has a clear understanding of the risks of money laundering and terrorist financing present in Andorra;
b) has access to all relevant information on the specific domestic and international risks associated with customers, products and services of the parties under obligation both on-site or off-site; and
c) bases the frequency and intensity of supervision on the risk profile of parties under obligation, and on the risks of money laundering and terrorist financing in Andorra, on-site and off-site.

4. The UIFAND may notify electronically its directives, circulars or explanatory notes and publish them in its website with full effectiveness.

5. The UIFAND reviews the adequacy and implementation of the internal policies, controls and procedures of the parties under obligation.

6. The UIFAND has access to the financial, administrative, judicial and law enforcement information required to fulfil their tasks properly. The UIFAND shall be able to respond to requests for information by Andorran competent authorities when such requests for information are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing. The decision on conducting the analysis or dissemination of information shall remain with the UIFAND.

7. Where there are objective grounds for assuming that the provision of such information would have a negative impact on ongoing investigations or analyses, or, in exceptional circumstances, where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested, the UIFAND shall be under no obligation to comply with the request for information.

8. Competent authorities shall provide feedback to the UIFAND about the use made of the information provided in accordance with this article and about the outcome of the investigations or inspections performed on the basis of that information.

Article 56. Composition of the UIFAND

1. UIFAND is composed of:

a) The members of UIFAND, formed by:
    i) the head of UIFAND;
    ii) a minimum of one person of recognised technical competence in the legal field;
    iii) a minimum of two people of recognised technical competence in the financial field;
    iv) a minimum of two people of recognised technical competence of the Department of Police;
b) the administrative personnel of UIFAND.

2. The Government determines by regulation the modalities relating to the organisation and functioning of UIFAND.

Article 57. Appointments

1. The head of the UIFAND is jointly appointed by the Ministers of Justice, Home Affairs and Finance, for a period of 6 years, renewable once.

The necessary requirements in order to be eligible for the position of head of the UIFAND are as it follows:

a) possession of a degree of level 4 of the Andorran Framework of higher education degrees in the field of law, economy or banking matters, granted or recognised by the Government;
b) broad proven knowledge of the regulations in matters of the detection, prevention of and fight against money laundering and terrorist financing;
c) proven experience in the detection, prevention of and fight against money laundering and terrorist financing, in the legal, financial or criminal investigation fields;
d) not being subject to any cause of incompatibility among those established in this Law.

2. The persons of recognised technical competence in the legal field and in the financial field are appointed by the Minister of Finance at the proposal of the head of the UIFAND.

The process of selecting them, handled by the UIFAND, and their employment relationship are governed by the Labour Law (Codi de relacions laborals) and the requirements of technical aptitude, merit and equality, and must respect the principles of objectivity, publicity and transparency.

3. In the event of the temporary absence or a conflict of interests of the head of the UIFAND, he delegates his functions or the function generating the conflict to another member of the UIFAND. This delegation is made in writing and signed by both parties, going into effect as from that time.

If, in the exercise of his functions, any other member of the UIFAND is faced with a possible conflict of interests, he communicates this circumstance immediately to the head of the UIFAND, who replaces him in the duty assigned and delegates the specific function to another member of the UIFAND.

4. The persons of recognised technical competence of the Department of Police are appointed by the Minister of Home Affairs at the proposal of the director of the Police and with the non-binding report of the head of the UIFAND.

5. The administrative personnel of the UIFAND is appointed according to the selection procedures established in the Civil Service Law. The head of the UIFAND is part of the selection process.

6. The composition of the UIFAND is published in the Official Gazette of the Principality of Andorra.

Article 58. Functions of the membres of the UIFAND

1. The head of the UIFAND is in charge of this administrative body and he is assigned the following functions:

a) administratively and technically manage and coordinate the UIFAND;
b) prepare the annual proposal of the budget of the UIFAND;
c) watch out for the security of the documentation and of the premises of the UIFAND and for the observance of the procedures and the compliance with the regulations by the members of the UIFAND and its administrative personnel;
d) act as the highest representative of the UIFAND before the parties under obligation, equivalent foreign bodies and national and international bodies which require his presence;
e) exercise any other function that may be assigned to him by this Law, by the regulations developing it and by the rest of the Law;

2. The members of the UIFAND act under the direction of the head of the UIFAND and exercise the functions that the head of the UIFAND assigns them, as well as those established by this Law and by its developing provisions.

Article 59. Termination of appointment

1. The head of the UIFAND terminates his appointment solely for one or more of the following causes:

a) termination of the period for which he has been appointed;
b) resignation, submitted in writing to the head or heads of the administrative bodies which have appointed him;
c) decease;
d) incapacity declared by firm court decision;
e) disqualification for the exercise of public offices declared by firm court decision;
f) conviction for the commission of an intentional crime;
g) serious breach of the obligations of his position;
h) ensuing incompatibility for the exercise of his position.

The Ministers of Justice, Home Affairs and Finance will be competent to determine, jointly and in a reasoned way, the termination of the appointment of the head of the UIFAND.

2. The termination of the appointment of the members of the UIFAND belonging to the Department of Police falls within the competence of the Minister of Home Affairs. The decision on their removal shall state the reasons in which it is grounded.

3. The termination of the appointment of the members of the UIFAND of recognised technical competence in the legal and financial field falls within the competence of the head of the UIFAND and it shall be carried out in compliance with the provisions of the Labour Law (Codi de relacions laborals). The decision on their removal shall state the reasons in which it is grounded.

4. The termination of the appointment of the administrative personnel of the UIFAND falls within the competence of the head of the UIFAND and it shall be carried out in compliance with the provisions of the Civil Service Law. The decision on their removal shall state the reasons in which it is grounded.

Article 60. Duty of secrecy

The members of the UIFAND and its administrative personnel are subject to secrecy in the employment sphere and to professional secrecy, during both the effective period of their relationship with the UIFAND and once this relationship has terminated.

Article 61. System of incompatibilities

1. The head of the UIFAND shall devote himself full time to the functions entrusted to him and he may not exercise any other professional activity in either the public sector or the private sector, except those expressly permitted in the system of incompatibilities of the Civil Service regulations.

In particular, the aforementioned position is incompatible with:

a) the exercise of any other public position attached to any of the institutions of the Public Administration, regardless of whether such position is by election, by appointment, in the civil service or under contract, except the positions which were to be the direct consequence of his status as head of UIFAND;
b) any directive or executive function or position in political parties;
c) generally, any activity that may jeopardise his independence, autonomy and impartiality in the fulfilment of his functions.

The breach of this system of incompatibilities will entail the removal of the head of the UIFAND from his position.

2. The members of the UIFAND belonging to the Department of Police are subject to the system of incompatibilities applicable to them in accordance with Qualified Law 8/2004, of 27 May, on the Department of Police.

3. The rest of the members of the UIFAND are subject to the system of incompatibilities which may be applicable to them, according to their type of employment, in compliance with the Civil Service Law.

Section 2. permanent committee for the prevention and fight against Money laundering and terrorist financing

Article 62. Nature

The Permanent Committee for the prevention and fight against money laundering and terrorist financing is a technical and advisory body of the Government in charge of coordinating the Andorran competent authorities in the field of the detection, prevention and fight against money laundering, and terrorist financing.

Article 63. Composition

1. The Permanent Committee for the prevention and fight against money laundering and terrorist financing is formed by the following members:

a) The head of the UIFAND, who chairs it, and three members of this unit appointed by their head, belonging each one to the different areas of expertise listed in points ii), iii) and iv) of paragraph 1 of article 56 of this Law.

b) The State Public prosecutor.
c) The director of the Police Department and the head of the unit of the Police Department responsible for the investigation of the cases of money laundering and terrorist financing.
d) The Director General of the Tax and Customs Department, or the deputy director to whom he may delegate.
e) When dealing with matters affecting the Andorran financial system and/or the insurance and reinsurance sector, a representative of the AFA, appointed by its Director General shall attend the meetings.
f) When dealing with matters affecting the external relations of the Principality of Andorra and, in any case, in relation to the functions of the Permanent Committee provided for in chapter IX of this Law, a representative of the Ministry of Foreign Affairs appointed by the Minister shall attend the meeting.
g) When dealing with matters affecting the Companies Register, the Associations Register or the Foundations Register, a representative of such registries shall attend the meeting as the case may be.
h) Occasionally, representatives of other bodies, departments, services, areas, advisors and representatives of professional bodies, Chamber of notaries or other entities which represent parties under obligation under this Law, may be called to deal with concrete items of the agenda.

2. The appointment of the designated members is valid until a new representative is appointed. Members not subject to appointment may delegate their functions.

Article 64. Subject-matter and functions

1. The Permanent Committee for the prevention and fight against money laundering and terrorist financing is aimed at coordinating the national competent authorities in the field of the detection, prevention and fight against money laundering, terrorist financing, and the proliferation of weapons of massive destruction and its financing.

2. In particular, the Permanent Committee for the prevention and fight against money laundering and terrorist financing, through its members, carries out the following functions:

a) participates in the analysis of the situation of money laundering in the Principality of Andorra, providing the available information, both statistical and observable in the performance of its functions;
b) participates in the assessment of the measures and actions carried out in the field of money laundering and terrorist financing;
c) offers advice on legislative changes;
d) attends international meetings;
e) provides advice on the drafting of reports addressed to international bodies;
f) those set out in chapter IX of this Law and, in particular, carries out the following functions:
    i) compiling and requesting, from any administration or party under obligation, directly or through their members, all information necessary to reasonably identify persons who meet the criteria to be included on the list set out by the United Nations Security Council from any relevant administration or party under obligation, either directly or through its members, and to identify persons and

entities that could reasonably be suspected of or believed to be involved in terrorism, terrorist financing, or of having an affiliation with organisations engaged in these activities;

ii) compiling and amending the list of persons associated with the activities described above, and adopting restrictive measures in accordance with the relevant provisions of this Law.

Article 65. Functioning

1. The Permanent Committee for the prevention and fight against money laundering and terrorist financing is chaired by the head of the UIFAND, who calls the meetings in due course by means of a letter to the representatives, sets the agenda and issues the respective minutes.

2. The Permanent Committee for the prevention and fight against money laundering and terrorist financing meets at least once every three months. Moreover, extraordinary meetings may be called whenever it is necessary in the judgement of the presidency or at the request of one or more members of the Permanent Committee for the prevention and fight against money laundering and terrorist financing; especially when a request is received from a State for a person or entity to be included on the list of persons and entities set out by chapter IX of this Law.

3. To formalise the request for an extraordinary meeting, a notice shall be written to the Chairman with the proposed agenda. Upon receipt of the request, the Chairman shall convene the meeting in due course.

4. Decisions are taken by a majority of the members on the Permanent Committee for the prevention and fight against money laundering and terrorist financing. In the event of a tie, the Chairman holds the deciding vote.

Chapter XI. Cooperation

Section 1. Internal cooperation

Article 66. Cooperation with judicial authorities

1. The UIFAND cooperates with judicial authorities in any kind of legal proceedings and in the execution of rogatory commissions related to acts of money laundering or terrorist financing.

Judicial authorities, ex officio or at the request of the Public Prosecutor's Office, make available, in a reasoned manner, information to the UIFAND when, in the course of a legal proceeding, indicia of non-compliance with this Law appear.

2. The Andorran authorities who discover facts that could constitute indicia or proof of money laundering or terrorist financing shall inform in writing the UIFAND and make available to it the information that the UIFAND requests in the exercise of its duties. Likewise, civil servants and other personnel in the service of the Andorran public administration that discover these facts shall make them known immediately to the body in which they work.

3. Information submitted in accordance with this article does not represent a breach of professional secrecy and confidentiality, and the authors shall avail themselves of the tutelage and protection established in article 26 of this Law.

4. The information and documents in possession or sent by the UIFAND in the exercise of its powers are strictly confidential. Any authority or officer who has access to such information and documents because of its position or powers has the duty to keep total secret.

Article 67. Cooperation with the Andorran Financial Authority (AFA)

1. The UIFAND informs the AFA, in its condition as the body that exercises the disciplinary power of the financial system and the insurance and reinsurance sector, of all transfer of files, whether to the Public Prosecutor's Office, or to the Government, when entities of the financial system or the insurance and reinsurance sector are implicated. This information includes the name of the entity under the supervision of the AFA, a description of the facts observed and the accounts mentioned in the file.

2. Likewise, the UIFAND and the AFA cooperate with reciprocity in the exercise of their functions of supervision and control, exchanging relevant information and experiences by written communications, regular meetings to follow up with the financial parties under obligation and their external auditors, and any other appropriate means to verify the effective fulfilment of the obligations imposed by the Andorran legal system.

In particular, when in the exercise of their supervisory functions the AFA notes possible infractions of the obligations established by the legislation for the prevention of money laundering and terrorist financing, the UIFAND shall be informed thereof.

3. In order to define the procedures of the cooperation regulated by this article, the UIFAND and the AFA may sign agreements of collaboration.

Section 2. International cooperation

Article 68. Cooperation between financial intelligence units

1. The UIFAND shall exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by other FIUs or equivalent bodies related to money laundering, its predicate offences, or terrorist financing and the natural or legal person involved, regardless of the type of predicate offences and even if the type of predicate offences is not defined at the time of the exchange..

Requests shall contain the relevant facts, background information, reasons for the request and how the information sought will be used.

When the UIFAND receives a suspicious transaction report which concerns another state, it shall promptly forward it to the FIU of that state.

2. The UIFAND shall use the whole range of its available powers which it would normally use domestically for receiving and analysing information when it replies to a request for information received from another FIU. The UIFAND shall respond in a timely manner.

Especially, when the UIFAND seeks to obtain additional information from a party under obligation established in another state which operates on its territory, the request shall be addressed to the FIU of the state in whose territory the party under obligation is established..

3. The exchange of information requires prior approval from the head of the UIFAND and is subject to the party receiving the information evidencing prior to receiving the information that it satisfies the following conditions:

a) reciprocity in the exchange of information;

b) the receiving state shall commit to not using the information for any other purpose than that sought by this Law; and

c) the foreign services receiving the information are bound, under threat of criminal sanction, by the duty of professional secrecy.

The UIFAND may refuse to exchange information where there are reasonable grounds to assume that the communication of this information may jeopardise ongoing investigations or analysis. The refusal of information shall be appropriately explained.

4. The UIFAND shall use secure channels to exchange information with other FIU.

5. Differences between national law definitions of predicate criminal offences shall not prevent the UIFAND from exchanging information or providing assistance to another FIU to the greatest extent possible under Andorran law, and shall not limit the use of information in the field of the prevention and fight against money laundering and terrorist financing.

Chapter XII. Sanctioning regime

Section 1. Infringements and sanctions

Article 69. Infringers or liable parties

1. Parties under obligation, natural or legal persons, are deemed to be infringers or liable parties when carrying out actions or omissions constituting an infringement under this Law, and provided that such infringement is attributable to their wilful misconduct or negligence.

2. In addition to the liability of the party under obligation, the persons holding senior management office within the latter shall be liable for any breach that is attributable to their wilful misconduct or negligence.

3. Natural or legal persons that fail to comply with the obligations established in paragraph 1 of article 19 of this Law.

Article 70. Categories of infringements

The administrative infringements provided for in this Law are classified as very serious, serious or minor.

Article 71. Very serious infringements

The following constitute very serious infringements if committed in a serious, repeated and systematic manner or a combination thereof:

1. Failure to comply with customer due diligence obligations relating to the identification or verification of customers or their beneficial owners.

2. Failure to comply with the obligation to establish adequate and sufficient internal control procedures when such failure implies a high risk of money laundering or terrorist financin.

3. Failure to comply with the suspicious transaction reporting duty in the terms established in article 20 of this Law.

4. Breach of freezing orders issued by the UIFAND in the terms established in paragraph 5 of article 20 of this Law.

5. Breach of the duty of confidentiality in the terms established in article 26 of this Law.

6. Breach of the prohibition on anonymous accounts and anonymous passbooks and with fictitious names established in article 7 of this Law.

7. Failure to comply with the obligation to submit to the UIFAND, in due time and form, all the information requested by the UIFAND in writing in the exercise of its functions, and all the information requested by the UIFAND to verify compliance with this Law and with the developing provisions in the terms established in point b) of paragraph 2 of article 55 of this Law.

8. Failure to comply with the obligation to report and adopt the restrictive measures established in articles 49 and 51 of this Law.

9. Resistance to or obstruction of, by action or omission, the supervisory function of the UIFAND, when there is an express written request in this respect.

10. Breach of the obligation to carry out an individual risk assessment (ERI) in the terms established in article 5 of this Law.

11. Failure to comply with the record-keeping obligations in the terms established in article 37 of this Law.

12. The commission of more than three serious infringements in a period of one year.

Article 72. Serious infringements

Són infraccions greus les següents:

1. Failure to comply with the special control obligation in the terms established in point g) of article 8 of this Law.

2. Failure to comply with the obligation to obtain information on the purpose and intended nature of the business relationship with the customer in the terms established in point c) of paragraph 1 of article 9 of this Law.

3. Failure to comply with the obligation of on-going monitoring of transactions and business relationships established in point d) of paragraph 1 of article 9 of this Law.

4. Failure to comply with the obligation not to establish or maintain business relationships in the terms established in paragraph 4 of article 10 of this Law or to carry out prohibited operations or transactions.

5. Failure to comply with the obligation of applying enhanced customer due diligence measures in the terms established in section 3 of chapter II of this Law.

6. Breach of the prohibition to establish or maintain correspondent banking relationships with shell banks in the terms established in article 13 of this Law.

7. Failure to comply with the obligations relating to wire transfers in the terms established in chapter V of this Law.

8. Failure to comply with the obligation to apply, with respect to branches, majority-owned subsidiaries or delegations of the financial parties under obligation located abroad, the measures provided for in article 41 of this Law.

9. Failure to comply with the obligation to carry out an annual external audit and to submit to the UIFAND the resulting audit report in the terms established in point a) of paragraph 1 of article 40 of this Law.

10. Failure to comply with the obligation to set up an internal control and communication body in the terms established in point b) of paragraph 1 and point a) of paragraph 2 of article 40 of this Law.

11. Failure to comply with the obligation to identify or verify the origin of the funds that are the object of the business relationship.

12. Failure to comply with the measures and obligations established in the First Additional Provision of this Law.

13. Failure to comply with the obligation to establish adequate and sufficient internal control procedures, when this does not constitute a very serious infringement.

14. Failure to comply with the technical communiqués issued by the UIFAND.

15. Breach of the obligation to carry out an appropriate, sufficient, objective and realistic individual risk assessment, when this does not constitute a very serious infringement.

16. The external auditor referred to in article 40 of this Law issuing an external audit report which is incomplete or has deficiencies.

17. Failure to comply with the measures and obligations established in the Third Additional Provision of this Law.

18. Failure to comply with the obligations established in paragraph 1 of article 19 of this Law.

19. The conducts specified in Article 71 of this Law, when they have not been committed in a serious, repeated or systematic manner.

20. The commission of more than three minor infringements within a period of one year.

Article 73. Minor infringements

Any breach of the provisions of this Law that is not specifically considered a serious or very serious infringement in the preceding articles.

Article 74. Sanctions aplicable to the parties under obligation which are legal persons

1. Very serious infringements are sanctioned with:

a) A fine ranging from EUR 90,001 to EUR 1,000,000.
b) A temporary or permanent restriction on specific types of transactions.
c) The withdrawal or modification of the corresponding activity authorisation.
d) A temporary or permanent prohibition to provide payment services.

The sanction provided for in point a) shall be imposed in all cases and may be simultaneously imposed with either one or both of the sanctions provided for in points b) and c).

2. Serious infringements are sanctioned with:

a) A fine ranging from EUR 15,001 to EUR 90,000.
b) A temporary restriction on specific types of transactions.

The sanction provided for in point a) shall be imposed in all cases and may be simultaneously imposed with the penalty provided for in point b).

3. Minor infringements are sanctioned with:

a) A written warning.
b) A fine ranging from EUR 600 to EUR 15,000.

The sanctions provided for in points a) and b) shall be imposed in all cases.

4. In addition to the sanction to be imposed on the party under obligation for the commission of the infringement, one or more of the following penalties may be imposed on those persons holding senior management office if the breach is attributable to their wilful misconduct or negligence:

a) In the case of very serious infringements: a fine ranging from EUR 25,001 to EUR 300,000 and/or a minimum temporary suspension from office of six months or permanent suspension from office.
b) In the case of serious infringements: a fine ranging from EUR 3,001 to EUR 25,000 and/or a temporary suspension from office of one to six months.
c) In the case of minor infringements: a written warning and/or a fine ranging from EUR 300 to EUR 3,000.

Article 75. Sanctions aplicable to parties under obligation who are natural persons

1. Very serious infringements are sanctioned with:

a) A fine ranging from EUR 25,001 to EUR 300,000.
b) A minimum temporary suspension of six months or permanent suspension.
c) A temporary or permanent restriction on specific types of transactions.
d) The withdrawal or modification of the corresponding activity authorisation.

The penalty provided for in point a) shall be imposed in all cases and may be simultaneously imposed with one or two or all of the penalties provided for in points b), c) and d).

2. Serious infringements are sanctioned with:

a) A fine ranging from EUR 3,001 to EUR 25,000.
b) A temporary suspension from office of one to six months.
c) A temporary restriction on specific types of transactions.

The penalty provided for in point a) shall be imposed in all cases and may be imposed simultaneously with one or both of the penalties provided for in points b) and c).

3. Minor infringements are sanctioned with:

a) A written warning.
b) A fine ranging from EUR 300 to EUR 3,000.

The fines provided for in points a) and b) shall be imposed in all cases.

Article 76. Exceptions to the ordinary sanctioning regime

1. Under no circumstances may the infringer benefit financially from the commission of an infringement.

2. When the financial benefit that the infringer obtains as a result of committing an infringement can be determined, the upper limit of the fine provided for in the preceding articles will be increased up to twice the aforementioned benefit, provided that the amount of the doubled benefit is higher than the upper limit.

3. When the infringer entity is a financial party under obligation, including the branches which carry out activities of the same nature in the Principality of Andorra, and the infringement has been serious, repeated and systematic, or has shown a combination of these characteristics, and such infringement is related to the customer due diligence obligations, the reporting of suspicious transactions, record-keeping, or the establishment of internal control procedures, the upper limit of the fine provided in the preceding articles may be raised:

a) In the case in which the infringer is a legal entity: up to 5% of the total annual turnover, proven by the latest available accounts approved by the governance body; or if the party under obligation is a parent company, or the subsidiary of a parent company, which draws up consolidated financial statements, the pertinent total turnover is the total annual turnover or the respective type of income, according to the most recent available consolidated financial accounts approved by the governance body of the ultimate parent company.

b) In the case in which the infringer is a natural person: up to 1,000,000 euros.

Article 77. Criteria for setting sanctions

L Sanctions are set according to any or all of the following criteria:

a) the degree of intention of the infringer.
b) the financial standing of the infringer.
c) the amount of the transaction and/or the profit obtained as a result of the infringement, and any losses caused to third persons by the infringement, to the extent that they may be determined.
d) the seriousness and duration of the facts.
e) the lack of monitoring and shortcomings or inadequacies in preventive mechanisms.
f) final sanctions imposed on the infringer in administrative proceedings in the last five years.
g) The cooperation of the infringer or responsible entity, with the UIFAND.

Article 78. Prescription

1. Infringements prescribe after three years. If measures are taken to disguise and conceal infringements from control or supervisory bodies, infringements prescribe after ten years.

The prescription period begins on the date on which the infringement is committed and, specificall:

a) for infringements arising from continuous activity, on the date of the termination of the activity or the last act with which the infringement is committed;
b) in the case of a breach of the customer due diligence obligations, on the date the business relationship ends;
c) in the case of a breach of the record-keeping obligation, at the end of the period referred to in article 37 of this Law.

The prescription period is interrupted when the UIFAND, with the formal knowledge of the parties under obligation, inspects, monitors or controls the compliance with the obligations set out in this Law. It is also interrupted by the initiation of sanctioning proceedings, with the knowledge of the party in question, or the initiation of legal proceedings based on the same facts.

The prescription period begins again following an interruption.

2. The action to enforce the sanctions prescribes after three years.

The prescription period begins on the day after the day on which the party is notified of the administrative decision by virtue of which the sanction becomes final.

If the administrative proceedings end due to negative administrative silence, the prescription period begins once the deadline to issue a decision has elapsed.

The prescription period is interrupted by the initiation, notified to the party in question, of the proceedings to enforce a sanction, and by the suspension of the enforcement of the sanctioning decision, granted in administrative or judicial proceedings.

Section 2. Sanctioning regime

Subsection 1. General provisions

Article 79. Regulation of the sanctioning proceedings

Before the sanctions established in this Law are imposed, sanctioning proceedings governed by the following provisions shall have been completed:

a) by the provisions set out in this section and the regulations, if any, developing them;
b) subsidiarily, by the Administrative Code and the other provisions governing sanctioning proceedings in administrative matters.

Article 80. Preliminary investigation

Before the initiation of sanctioning proceedings, a preliminary investigation may be carried out in order to preliminary determine whether there are circumstances that justify the same. In particular, a preliminary investigation shall aim to determine, as precisely as possible, the facts justifying the initiation of the proceedings, the identification of the person or persons who may prove to be liable, and all relevant circumstances in this respect.

Article 81. Initiation of the proceedings

1. The sanctioning proceedings begin with an order from the UIFAND, issued at its own initiative, following a reasoned request from other bodies, or in response to an accusation. By means of this order, the UIFAND only:

a) orders the initiation of the sanctioning proceedings;
b) makes a brief reference to the facts, including by referral to a prior inspection report or to a prior accusation;
c) identifies, if possible, the allegedly liable person or persons;
d) appoints an investigator. This investigator shall be a member of the UIFAND.

2. The sanctioning proceedings is communicated to the investigator and notified to the allegedly liable person or persons so that they are aware of the initiation of the sanctioning proceedings and may challenge the appointment of the investigator within ten days.

3. The appointment of the investigator is subject to the provisions on abstention and recusal established in the Administrative Code.

4. If the appointed investigator is absent or temporarily unavailable, the UIFAND will appoint a new investigator.

5. The UIFAND shall notify the initiation of the sanctioning proceedings to the Government and, in the event that the allegedly liable persons are entities operating in the financial system or in the insurance and reinsurance sector, it shall also notify the AFA.

Article 82. Links with the criminal jurisdiction

1. If at any time during the administrative sanctioning proceedings it becomes apparent that the facts may constitute a criminal offence, the UIFAND shall immediately report such circumstance to the Public Prosecutor's Office.

The Public Prosecutor's Office shall notify the UIFAND both if it decides not to bring a criminal prosecution and if it decides to do so, and moreover, when the latter takes place, the result of such prosecution.

2. If at any time during the administrative sanctioning proceedings it is evidenced that criminal proceedings have been initiated for the same facts, the administrative proceedings shall be suspended until a judgment in the criminal proceedings becomes final.

3. The competent body to impose the sanctions shall not impose any administrative sanction and shall shelve the proceedings if, before issuing the decision, it has been evidenced that a final criminal sanction has been imposed based on the same facts and grounds.

Article 83. Precautionary measures

1. Once the proceedings have been initiated and at any time during such proceedings, the UIFAND may order the precautionary measures it deems appropriate in order to ensure the enforceability of any decision that is issued, as long as there is sufficient evidence of an infringement.

2. These measures may consist of: provisionally banning the performance of specific types of financial or commercial transactions; ordering the provisional suspension from office of persons who, due to their holding senior management office within the parties under obligation, appear as allegedly liable parties for very serious infringements.

3. The precautionary measures shall be proportional to the intended purpose and shall be lifted as soon as no longer serve such purpose..

4. An appeal may be lodged against the decision of the UIFAND before the Administrative Section of the Tribunal de Batlles (first instance collegiate court), within thirteen working days from the day after the notification of the adopted measure.

The judicial appeal does not suspend enforcement, in accordance with the Administrative Code, unless the Administrative Section of the Tribunal de Batlles (first instance collegiate court) exercises its discretionary powers according to the Administrative Code and concordant rules.

Article 84. Investigation stage

The investigator shall order the performance of all the actions and the gathering of all the evidence that he deems appropriate to clarify the facts of the case and to determine the outstanding liabilities.

The investigator shall draft a report setting out the conclusions of the investigation.

Article 85. Statement of charges

1. At the end of the investigation stage, and in view of the actions carried out, the investigator shall draft a statement of charges with the following minimum content:

a) Identity of the party or parties, natural or legal entities, who are liable, including the persons holding senior management office and to whose wilful misconduct or negligence the commission of the infringement is attributable, as appropriate.
If more than one person is involved, the facts attributed to each one of them shall be specified.
b) A brief statement of the facts that justify the initiation of the sanctioning proceedings, how they are classified with reference to the infringed provisions, and the proposed sanctions.
The statement of charges may refer to the investigation report as long as the investigation report and the statement of charges contain all the elements listed in this point.
c) Right of the allegedly liable party to examine the file, to file allegations, to submit documents, to propose evidence and the term for exercising these rights.
If the investigator considers that no administrative infringement has been committed, he will not issue a statement of charges and will instead forward a reasoned recommendation to the UIFAND that the latter shelve the proceedings.

2. The statement of charges shall be notified to the alleged infringers, who have a period of ten days from the day after the notification to file the allegations that they deem appropriate and to propose the proof, if any, that they deem appropriate or to make the voluntary payment of the proposed fine with a 25% reduction.

If the fine is paid in the terms established in this Law, the summary sanctioning proceeding will apply; otherwise, the ordinary sanctioning proceeding will apply.

3. In view of the allegations filed and the proof proposed by the alleged infringers, the investigator may decide, ex officio, to open an examination period in the terms established in the Administrative Code.

4. Copies of the administrative sanctioning file should be provided and the alleged infringers given access to it when the statement of charges is notified.

Subsection 2. Summary sanctioning proceeding

Article 86. Summary sanctioning proceeding

1. Once the party in question has voluntarily paid the proposed fine with a 25% reduction, this party will notify the UIFAND of the payment within the deadline set out in paragraph 2 of the previous article. This voluntary payment has the following effects:

a) waiver of the right to file allegations against the statement of charges.
b) the infringer's full agreement and acceptance of the alleged facts and infringements, the commission of which is acknowledged, together with the legal arguments justifying the sanction.
c) regardless of the type of sanction, the statement of charges will be considered to be a sanctioning decision, which will be final from the moment in which the fine is paid.

2. The voluntary payment of the fine proposed in the statement of charges in the terms established in this Law entails, together with the 25% reduction of the fine, a 25% reduction in the period of temporary suspension from office of the person(s) holding senior management office within the structure of the party under obligation that is proposed in the statement of charges.

3. Lodging any type of administrative or judicial appeal against the statement of charges, as a sanctioning decision, entails the appellant's waiver of the 25% reduction in any temporary suspension from office of the person(s) holding senior management office within the structure of the party under obligation, as well as the 25% reduction in the fine imposed, which the appellant shall pay within three days after lodging the appeal. Once this period has expired, enforcement action may be taken to obtain payment.

Subsection 3. Ordinary sanctioning proceeding

Article 87. Draft decision

1. Once the allegations have been filed against the statement of charges or the period for their submission has expired, and all the additional actions deemed appropriate by the investigator have been carried out, the investigator:

a) formulates a draft decision which sets out the facts (and evidence of them), how they are classified, the attributed infringement or infringements, the party or parties considered liable, and the proposed sanction, or
b) proposes the dismissal and shelving of the case.

2. The draft decision, together with all the elements of the file, shall be forwarded to the UIFAND so that it may decide on the case or forward it to the competent body for a final decision.

Article 88. Decision

1. The Government is competent to impose administrative sanctions relating to serious and very serious infringements.

Only if the draft decision of the UIFAND proposes the withdrawal or modification of an activity authorisation shall the Government notify the draft decision to the competent body for granting the aforementioned authorisation so that it may issue a binding report, within three months, in which a decision is made on said withdrawal or modification of the authorisation.

The enforcement of the final sanctions consisting of the withdrawal or modification of activity authorisations corresponds to the body that grants the authorisation.

2. The UIFAND is competent to impose administrative sanctions relating to minor infringements.

3. The competent body to decide on the case, by means of reasoned decision notified to the infringer, shall set out the facts which it considers proven, the statutory provision defining the infringement, and the statutory provision setting out the sanction imposed.

4. If the infringer is an operative entity of the financial system, the competent body to decide on the case shall notify the sanctioning decision to the Andorran Financial Authority.

Article 89. Expiration of the proceeding

1. The deadline for deciding and notifying the decision to the infringers is two years from the notification of the sanctioning proceedings to the alleged liable party or parties, without prejudice to a possible extension of six additional months that may be granted by the UIFAND, if justified, at the proposal of the investigator, and notified to the infringer.

If this period lapses without any express decision having been notified for reasons attributable to the authorities, the proceedings will expire.

2. The deadline for issuing a decision in sanctioning proceedings and for notifying the sanctioning decision to the infringer is suspended in the following cases:

a) when an opinion or report from another body is requested, for the time from the request being made, which shall be notified to the liable parties, to the notification of the resulting opinion or report to the UIFAND. A suspension for this reason may not exceed three months;
b) when proceedings based on the same facts are filed before any judicial body, until the decision of the competent judicial body becomes final;
If the UIFAND reports to the Public Prosecutor's Office that the facts may constitute a criminal offence, the sanctioning proceedings are suspended from the date on which the UIFAND reports to the Public Prosecutor's Office until, depending on the case, the communication of the Public Prosecutor's Office to the UIFAND of its decision not to bring a criminal prosecution or until the decision of the corresponding judicial body becomes final.
c) when, within the framework of sanctioning proceedings, urgent and preferential proceedings are initiated in the terms established in article 41.1 of the Constitution, and until the decision of the corresponding judicial body becomes final.

3. The expiration of the proceedings may be declared ex officio or at the request of the party in question, and the declaration will order the shelving of the case.

4. The expiration of administrative proceedings does not prevent the initiation of new proceedings on the basis of the same facts and legal grounds, as long as the infringement in question has not prescribed.

Article 90. Appeal

Sanctioning decisions bring the administrative proceedings to an end. An appeal may be lodged against sanctions before the Administrative Section of the Tribunal de Batlles (first instance collegiate court), within thirteen working days from the day after the notification of the decision.

Section 3. Whistleblowing

Article 91. Whistleblowing

1. The UIFAND sets out, by means of a technical communiqué, mechanisms to encourage the reporting of potential or actual breaches of this Law and its developing provisions.

2. The mechanisms referred to in paragraph 1 shall include at least:

a) specific procedures for the receipt of reports on breaches and their follow-up;
b) appropriate protection for employees or persons in a comparable position, of parties under obligation who report breaches committed within the party under obligation;
c) appropriate protection for the accused person;
d) protection of personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach;
e) clear rules that ensure that confidentiality is guaranteed in all cases in relation to the person who reports the breaches committed within the party under obligation, unless disclosure is required in the context of further investigations or subsequent judicial proceedings.

3. Parties under obligation shall have in place appropriate procedures for their employees, or persons in a comparable position, to report breaches internally through a specific, independent and anonymous channel, proportionate to the nature and size of the party under obligation concerned.

4. Individuals who are exposed to threats, retaliation or hostile actions, or adverse or discriminatory employment actions for whistleblowing as referred to in this article, are entitled to file a complaint before the UIFAND, which shall analyse and, in the event of finding evidence or verifying the existence of a criminal offence, report it to the Public Prosecutor.

Provisions

First additional provision. Non-profit organizations

1. The board of directors, the surveillance body, the board of trustees, or the pertinent representation body that manages the interests of the organization, and the personnel of same with management responsibilities, shall ensure that these organizations are not used for money laundering or to channel funds or resources to persons and entities linked to terrorist groups or organizations, in accordance with the provisions on the prevention and fight against money laundering and terrorist financing.

To this end, all organizations shall keep, for ten years, records with the identity of all the persons who receive funds or resources from the organization, and, in the case of associations, shall also keep the record books which are referred to in Article 28 of the Qualified Law of Associations. These registers and books shall be at the disposal of the administrative or judicial bodies with competences in the field of the prevention and fight against money laundering, and terrorism and its financing, as well as at the disposal of the persons in charge of the Register of Associations, when aplicable.

2. The scope of the obligations established in this provision may be developed by regulatory mean.

Second additional provision. Communication of activity

1. Professionals who, whether by acting on behalf of and for their clients, or by assisting in the planning or carrying out of transactions for their clients concerning the:

- organisation of contributions necessary for the creation, operation or management of companies;
- creation, operation or management of trusts, companies, associations, foundations, or similar structures;

and that are not registered in a professional body officially recognised for the exercise of its activity shall communicate to the Ministry of Economy, prior to the exercise of the activity, the activities they are seeking to exercise of those listed in this paragraph.

2. This communication is an essential requirement to carry out, on behalf of and for their clients, the activities above mentioned.

The Ministry competent in foreign investment shall verify compliance with the communication obligation set out in paragraph 1 and shall deny any foreign investment request consisting of any of the above mentioned activities if the professional who acts on behalf of and for his clients has not complied with that obligation.

3. Notaries are not subjected to the communication obligation set out in paragraph 1.

Third additional provision. Persons who exercise functions of trustee or an equivalent position

1. The natural persons or legal entities that exercise functions of trustee or an equivalent position in legal structures similar to trusts, of professional or non-professional nature, are subject to the following measures:

a) they are to keep the following updated information on the trust:
   i) the beneficial owners;
   ii) the residence of the trustee or of the analogous figure;
   iii) any assets held or managed by a financial or non-financial party under obligation.
b) they are to keep the documents, data and information within the framework of the procurement of the information required in the preceding letter, according to the terms established by Article 37 of this Law, and to communicate it to the competent authorities as soon as it were to be requested;
c) when they establish a business relationship or carry out an occasional transaction, they are to communicate their status to the financial institutions and to other non-financial parties under obligation, as well as the updated information with respect to:
   i) the beneficial owners;
   ii) the residence of the trustee or of the analogous figure;
   iii) any assets held or managed by a financial or non-financial party under obligation.

2. The operation, provision of information and access to the Register of Trust and Similar Legal Arrangements Service Providers is developed by regulations.

Fourth additional provision. Register of Financial and Assimilated Accounts

1. Banking entities, payment service providers and electronic money service providers operating in the Principality of Andorra shall report to the Register of Financial and Assimilated Accounts the identity of holders or beneficial owners of payment accounts or bank accounts identified by IBAN, and safe-deposit box lease agreements and their lease period, regardless of their commercial name. The reports shall not include accounts and safedeposit boxes in branches abroad.

The reported information shall be registered in the Register of Financial and Assimilated Accounts of the Ministry of Finance, which is in charge of processing it in accordance with the data protection rules.

2. The UIFAND shall have direct, immediate and unfiltered access to the information recorded in the Register, without any restriction.. This information will also be accessible to the competent national authorities for the prevention, detection, investigation and prosecution of money laundering and other related criminal offences, in order to comply with obligations under this Law.

Access to information in the Registry shall identify the person/s or the account number in relation to which information is requested. Generic and proximity searching is not admissible.

The access system shall maintain a detailed register of consultations, and, at least, shall record:

a) the user ID of the authority or public official accessing the Register and requesting information and, if applicable, the authority or public official that orders the request for information and the recipient of the results;
b) the type of data used to initiate the request;
c) the date and time of the request;
d) the reason or grounds for the request with express reference to the proceedings to which they relate;
e) the identifier of the results.

The scope of the access requirements established in this provision may be developed by regulations.

3. Reporting by banking entities, payment services providers and electronic money service providers will contain the following information, which shall be accessible through the Register of Financial and Assimilated Accounts:

a) in relation to the customer-account holder and safe-deposit box lessees and any person purporting to act on behalf of the customer:
    i) in the case of natural persons; name and surname, date and place of birth, nationality, address, country or countries of residence, tax identification number or equivalent, passport number or equivalent;
    ii) in the case of legal persons, trusts and other similar legal instruments: name, legal form, registered address, and, if different, the place of its principal establishment or business, tax identification number or equivalent;

b) in relation to the beneficial owner(s) of the bank account or safe-deposit box lease: name and surname, date and place of birth, nationality, address, country or countries of residence, tax identification number or equivalent, passport number or equivalent;
c) in relation to bank or payment accounts: the IBAN number and dates the account was opened and closed;
d) in relation to safe-deposit box leases: the number of the lease agreement or its internal identification number; the duration of the lease.

The reporting shall be done electronically in the terms and with the frequency established by the regulations and according to the template report attached to the regulations.

Fifth additional provision. Access to information on real estate in Andorra

The UIFAND may access, in the performance of their duties, notarial and cadastral information and documentation that identifies any natural or legal person or any trust or similar legal instrument owning real estate in the Andorran territory. This information will also be accessible to the national authorities competent in the field of the prevention, detection, investigation and prosecution of money laundering and other criminal offences, in order to comply with the obligations imposed by this Law.