Law of 12 November 2004 on the fight against money laundering and terrorist financing

coordinated version as of 25 May 2021

Please note that this is a non-official translation drawn up by Arendt & Medernach for information purposes only. In case of discrepancies between the French and the English texts, the French text, as published in the *Mémorial*, the Luxembourg official journal, shall prevail. Coordinated version as of the law of 20 May 2021, published in the *Mémorial* A N° 384 of 21 May 2021.

Arendt & Medernach SA
Registered with the Luxembourg Bar
RCS Luxembourg B 186371

arendt.com

41A avenue JF Kennedy
L-2082 Luxembourg
T +352 40 78 78 1

Law of 12 November 2004 on the fight against money laundering and terrorist financing

TITLE I

Professional obligations concerning the fight against money laundering and terrorist financing

Chapter 1: Definitions, scope and designation of supervisory authorities and self-regulatory bodies

Art. 1. Definitions

(1) "Money laundering" means, for the purposes of this law, any action as defined in Articles 506-1 of the Penal Code and 8-1 of the law of 19 February 1973 on the sale of medicinal substances and the fight against drug addiction, as amended.

(1a) The term "associated underlying offence" refers to the offences referred to in Article 506-1 point (1) of the Penal Code and in Article 8 paragraph (1)(a) and (b) of the law of 19 February 1973 on the sale of medicinal substances and the fight against drug addiction, as amended.

(2) "Terrorist financing" means, for the purposes of this law, any action as defined in Article 135-5 of the Penal Code.

(3) "Credit institution" means, for the purposes of this law, any credit institution within the meaning of point 1 of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, including its branches, within the meaning of point 17 of Article 4(1) of that Regulation, whether its head office is situated in the Union or in a third country.

(3a) "Financial institution" means, for the purposes of this law:

(a) any insurance undertaking within the meaning of point (1) of Article 13 of Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance in so far as it carries out life insurance activities governed by that Directive;

(b) any investment firm within the meaning of point (1) of Article 4(1) of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU;

(c) any undertaking for collective investment which markets its units or shares;

(d) any insurance intermediary within the meaning of point (3) of Article 2(1) of Directive (EU) 2016/97 of the European Parliament and of the Council of

20 January 2016 on insurance distribution, when engaged in life insurance and other investment-related services;

(e) any undertaking other than those referred to in points (a) to (d), as well as paragraph (3), which carries out one or more of the activities listed in Annex I in a professional capacity, for or on behalf of a customer;

(f) any branch in Luxembourg of the financial institutions referred to in points (a) to (e) and (g), whether its head office is located in a Member State or in a third country.

(g) any undertaking that the CSSF is responsible for supervising with respect to its professional anti-money laundering and counter-terrorist financing obligations in accordance with Article 2-1 (1).

(3b) "Group" means, for the purposes of this law, any group of undertakings comprising a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC, hereinafter "Directive 2013/34/EU".

(4) "Member State" means, for the purposes of this law, a Member State of the European Union. The States that are contracting parties to the European Economic Area Agreement other than the Member States of the European Union, within the limits set forth by this agreement and related acts, are considered as equivalent to Member States of the European Union. "Another Member State" means a Member State other than Luxembourg.

(5) "Third country" means, for the purposes of this law, a State other than a Member State.

(6) "Property" means, for the purposes of this law, assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible; and legal documents or instruments in any form, including electronic or digital, evidencing title to or an interest in such assets.

(7) "Beneficial owner" means, for the purpose of this law, any natural person who ultimately owns or controls the customer or any natural person on whose behalf a transaction or activity is carried out. The concept of beneficial owner shall at least include:

(a) in the case of corporate entities:

(i) any natural person who ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or an ownership interest in that entity, including through bearer shareholdings or control by other means, other than a company listed on a regulated market that is subject to disclosure requirements

consistent with European Union law or subject to equivalent international standards that ensure adequate transparency of information relating to ownership.

A shareholding of 25% of the shares plus one share, or an ownership interest of more than 25% in the customer's share capital, held by a natural person, shall be an indication of direct ownership. A shareholding of 25% of the shares plus one share, or an ownership interest of more than 25% in the customer's share capital, held by a legal person which is controlled by one or more natural persons, or by several companies which are controlled by the same natural person(s), shall be an indication of indirect ownership.

(ii) any natural person who holds the position of senior managing official if, after having exhausted all possible means and provided there are no grounds for suspicion, none of the persons referred to in point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owners(s).

Other means of control may be determined in accordance with Articles 1711-1 to 1711-3 of the law of 10 August 1915 on commercial companies, as amended, or where the following criteria are present:

(aa) a direct or indirect right to exercise a dominant influence over the customer pursuant to an agreement concluded with it or pursuant to a provision of its articles of association, where the law governing the customer permits it to be bound by such agreements or provisions;

(bb) where, during both the current and previous financial years and up until the drafting of the consolidated financial statements, the majority of the members of the customer's administrative, management or supervisory bodies have been appointed as a direct or indirect result of the exercise of a single natural person's voting rights;

(cc) a direct or indirect power to exercise, or the actual direct or indirect exercise of, a dominant influence or control over the customer, including the fact that the customer shares the management structure of another company;

(dd) an obligation under the national law governing the customer's parent company to draft annual consolidated financial statements and a consolidated management report;

(b) in the case of *fiducies* and trusts, any of the following persons:

(i) the settlor(s);

(ii) the *fiduciaire(s)* or trustee(s);

(iii) the trust protector(s), where applicable;

(iv) the beneficiaries or, where the persons benefiting from the legal arrangement or legal person have not yet been designated, the category

of natural persons in whose main interest the legal arrangement or legal person is set up or operates;

(v) any other natural person exercising ultimate control over the *fiducie* or 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 *fiducies* or trusts, any natural person holding equivalent or similar positions to those referred to in point (b).

(8) For the purposes of this law, "trust and company service provider" means any natural or legal person which provides, in a professional capacity, any of the following services to third parties:

(a) forming companies or other legal persons;

(b) acting as director or secretary of a company, as partner in a partnership, or holding a similar role with regard to other types of legal person, or arranging for someone else to fulfil such a role;

(c) providing a registered office, business address, correspondence or administrative address or professional premises and other related services for a company, a partnership or any other legal person or similar legal arrangement;

(d) acting as or arranging for another person to act as a *fiduciaire* in a *fiducie* or trustee of an express trust or an equivalent function in a similar legal arrangement;

(e) acting as a shareholder on behalf of another person or arranging for someone else to fulfil such a role.

(9) For the purposes of this law, "politically exposed persons" (PEPs) means natural persons who are or have been entrusted with prominent public functions and their family members, or persons known to be close associates of such persons.

(10) In accordance with paragraph (9) above, "natural persons who are or have been entrusted with prominent public functions" means any of the following natural persons:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or members of similar legislative bodies;

(c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal except in exceptional circumstances;

(d) members of courts of auditors, or of the boards or management boards of central banks;

(e) ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces;

(f) members of the administrative, management or supervisory bodies of State-owned enterprises;

(g) officials and members of governing bodies of political parties;

(h) directors, deputy directors and members of the board, or those holding an equivalent position, in an international organisation.

(i) natural persons in roles appearing on the list published by the European Commission on the basis of Article 20a(3) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, hereinafter "Directive (EU) 2015/849".

None of the categories set out in (a) to (h) above shall be understood as including middle-ranking or more junior officials.

(11) In accordance with paragraph (9), "family members" refers to any of the following physical persons, including, in particular:

(a) the spouse;

(b) any partner considered by national law as equivalent to the spouse;

(c) children and their spouses or partners considered by national law as equivalent to the spouse;

(d) parents;

(e) siblings.

(12) In accordance with paragraph (9) above, "persons known to be close associates" means any of the following natural persons:

(a) any natural person who is known to have joint beneficial ownership of legal persons or legal arrangements, or any other close business relations, with a person referred to in paragraph (10);

(b) any natural person who has sole beneficial ownership of a legal person or legal arrangement which is known to have been set up for the de facto benefit of the person referred to in paragraph (10).

(13) For the purposes of this law, "business relationship" means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by this law and which is expected, at the time when the contact is established, to have an element of duration.

(14) For the purposes of this law, "shell bank" means a credit institution, or a financial institution, or an institution engaged in equivalent activities, that is incorporated or

authorised in a jurisdiction or territory in which it has no physical presence involving meaningful mind and management, and that is unconnected or unaffiliated with a regulated financial group.

(15) "Persons engaging in a financial activity on an occasional or very limited basis" means natural or legal persons who engage in a financial activity which fulfils the following criteria:

(a) the financial activity is limited in absolute terms and does not exceed a sufficiently low threshold set up by Grand Ducal regulation depending on the type of financial activity;

(b) the financial activity is limited as regards transactions and does not exceed a maximum threshold per customer and per transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked, this threshold being set up by Grand Ducal regulation according to the type of financial activity at a sufficiently low level in order to ensure that the types of transactions in question are an impractical and inefficient method for laundering money or for terrorist financing, and shall not exceed EUR 1,000;

(c) the financial activity is not the main activity, the turnover of the financial activity in question does not exceed 5% of the total turnover of the natural person or legal person concerned;

(d) the financial activity is ancillary and directly related to the main activity;

(e) the main activity is not an activity exercised by professionals listed in Article 2(1), with the exception of activities of such persons referred to in point (15) of Article 2(1);

(f) the financial activity is provided only to the customers of the main activity and is not generally offered to the public.

(16) "Supervisory authority" means, for the purposes of this law, each of the authorities referred to in Article 2-1(1), (2) and (8).

(17) "European Supervisory Authorities" means, for the purposes of this law, the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority.

(18) "Payable-through account" means, for the purposes of this law, any correspondent account used directly by third parties to carry out transactions on their own behalf.

(19) "Member of the senior management" means, for the purpose of this law, any director (*dirigeant*) or employee with sufficient knowledge of the professional's money laundering and terrorist financing risk exposure and who holds a sufficiently senior position to take decisions affecting that risk exposure, and need not, in all cases, be a member of the board of directors.

(20) "Electronic money" means, for the purposes of this law, electronic money within the meaning of point (29) of Article 1 of the law of 10 November 2009 on payment services, as amended.

(20a) "Virtual currency" means, for the purposes of this law, a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of a currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically.

(20b) "Virtual asset" means, for the purposes of this law, a digital representation of value, including virtual currency, that can be digitally traded or transferred, and can be used for payment or investment purposes, with the exception of virtual assets which meet the description of electronic money within the meaning of point (29) of Article 1 of the law of 10 November 2009 on payment services, as amended, and virtual assets which meet the description of financial instruments within the meaning of point (19) of Article 1 of the law of 5 April 1993 on the financial sector, as amended.

(20c) "Virtual asset service provider" means, for the purposes of this law, any person that provides, for or on behalf of a customer, one or more of the following services:

(a) exchange between virtual assets and fiat currencies, including exchange between virtual currencies and fiat currencies;

(b) exchange between one or more forms of virtual assets;

(c) transfer of virtual assets;

(d) safekeeping or administration of virtual assets or instruments enabling control over virtual assets, including custodian wallet services;

(e) participation in and provision of financial services related to an issuer's offer or sale of a virtual asset.

(20d) "Safekeeping or administration service provider" means, for the purposes of this law, the safekeeping or administration service provider of virtual assets or instruments enabling control over virtual assets, including custodian wallet providers.

(20e) "Custodian wallet services" means, for the purposes of this law, services to safeguard private cryptographic keys on behalf of customers, in order to hold, store and transfer virtual currencies.

(21) "Self-regulatory body" means, for the purposes of this law, a body composed of members of a profession which it represents, which has a role in regulating them, in performing certain supervisory or monitoring type functions and in ensuring the enforcement of the rules relating to them. Each of the bodies referred to in Article 2-1(3) to (7) shall be so designated.

(22) "Correspondent relationship" means, for the purpose of this law:

(a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including 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) any similar relationship between and among credit institutions and financial institutions including where services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

(23) "Gambling services" means, for the purposes of this law, services which involve wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at physical locations, or by any means at a distance, by electronic means or any other technology intended to facilitate communication, and at the individual request of a recipient of services, save for games that do not give the player any chance of enrichment or material benefit other than the right to continue playing.

(24) "Professionals" means, for the purposes of this law, all persons referred to in Article 2.

(25) "CSSF" means, for the purposes of this law, the *Commission de surveillance du secteur financier*.

(26) "CAA" means, for the purposes of this law, the *Commissariat aux assurances*.

(27) "AED" means, for the purposes of this law, the Registration duties, Estates and VAT authority (*Administration de l'enregistrement, des domaines et de la TVA*).

(28) "FIU" means, for the purposes of this law, the Financial Intelligence Unit.

(29) "Person" means, for the purposes of this law, a natural person or legal person, as the case may be.

(30) "High-risk country" means, for the purposes of this law, a country included in the list of high-risk third countries established pursuant to Article 9(2) of Directive (EU) 2015/849 or designated as presenting a higher risk by the Financial Action Task Force (FATF), as well as any other country considered by supervisory authorities and professionals, in the context of their assessments of the risks of money laundering and terrorist financing, to be a high-risk country based on the geographical risk factors listed in Annex IV.

Art. 2. Scope

(1) This title applies to the following persons:

1. credit institutions and professionals of the financial sector (PSFs) licensed or authorised to carry out their business in Luxembourg pursuant to the law of 5 April 1993 on the financial sector, as amended, and payment institutions and electronic money institutions licensed or authorised to carry out their business in Luxembourg pursuant to the law of 10 November 2009 on payment services, as well as tied agents as defined in Article 1 of the law of 5 April 1993 on the financial sector, as amended and agents as defined in Article 1 of the law of 10 November 2009 on payment services, established in Luxembourg;

1a. The natural and legal persons benefiting from the waiver in accordance with Article 48 or 48-1 of the law of 10 November 2009 on payment services;

2. insurance undertakings licensed or authorised to exercise their activities in Luxembourg in accordance with the law of 7 December 2015 on the insurance sector, as amended, in connection with operations under Annex II of the law of 7 December 2015 on the insurance sector, as amended and insurance intermediaries licensed or authorised to exercise their activities in Luxembourg in accordance with the law of 7 December 2015 on the insurance sector, as amended when they act in respect of life insurance and other investment related services;

2a. Professionals of the insurance sector authorised to exercise their activities in Luxembourg pursuant to the law of 7 December 2015 on the insurance sector, as amended;

3. pension funds under the prudential supervision of the Commissariat aux assurances;

4. undertakings for collective investment and investment companies in risk capital (SICAR), which market their units, securities or partnership interests and to which the law of 17 December 2010 on collective investment undertakings, as amended, or the law of 13 February 2007 on specialised investment funds or the law of 15 June 2004 on investment companies in risk capital (SICAR) applies;

5. management companies referred to in the law of 17 December 2010 on collective investment undertakings, as amended and alternative investment fund managers subject to the law of 12 July 2013 on alternative investment fund managers, as amended;

6. pension funds subject to prudential supervision by the *Commission de surveillance du secteur financier*;

6a. managers and advisors of undertakings for collective investment, investment companies in risk capital (SICAR) and pension funds;

6b. securitisation undertakings, where they perform trust and company service provider activities;

6c. insurance and reinsurance undertakings and their intermediaries, where they perform credit and surety operations;

(…)[1]

6e. any person exercising the activity of Family Office within the meaning of the law of 21 December 2012 on the activity of Family Office;

7. other financial institutions exercising their activities in Luxembourg;

[1] Repealed by the law of 25 March 2020 – AML 5.

8. *réviseurs d'entreprises*, *réviseurs d'entreprises agréés*, audit firms and *cabinets de révision agréés* (approved audit firms) within the meaning of the law of 23 July 2016 on the audit profession, as amended;

9. accountants, within the meaning of the law of 10 June 1999 on the organisation of the accounting profession;

9a. accounting professionals, within the meaning of point (d) of Article 2(2) of the law of 10 June 1999 on the organisation of the accounting profession;

10. real estate agents, within the meaning of the law of 2 September 2011 governing access to the professions of skilled craftsman, trader and manufacturer, as well as to certain liberal professions, as amended, established or active in Luxembourg, including when acting in the capacity of intermediary for the rental of immoveable property, but only with respect to transactions for which rent is at least EUR 10,000 per month;

10a. property developers, within the meaning of the law of 2 September 2011 governing access to the professions of skilled craftsman, trader and manufacturer, as well as to certain liberal professions, as amended, established or active in Luxembourg, including when acting in the capacity of intermediary involved in the transactions entailing the purchase or sale of immoveable property;

11. notaries, within the meaning of the law of 9 December 1976 on the organisation of the profession of notary, as amended;

11a. bailiffs, within the meaning of the law of 4 December 1990 on the organisation of the service of court bailiffs, as amended, where they carry out valuation and public sales of furniture, moveables and harvests;

12. lawyers, within the meaning of the law of 10 August 1991 on the legal profession, as amended, when:

    (a) assisting in the planning or execution of transactions for their customer concerning the:

        (i) buying and selling of immovable property or business entities,

        (ii) managing client money, securities or other assets,

        (iii) opening or managing bank, savings or securities accounts,

        (iv) organising the necessary contributions for the creation, operation or management of companies,

        (v) performing the creation, domiciliation, operation or management of trusts, companies or other similar structures,

    (b) or acting for and on behalf of their customer in any financial or real estate transaction;

(c) or providing a service of a trust and company service provider;

(d) or exercising the activity of Family Office.

13. persons other than those listed above who:

(a) carry out, by way of its business, tax consulting activities in Luxembourg;

(b) carry out, by way of its business, in Luxembourg, any of the activities described in 12(a) and (b); or

(c) undertake to provide, directly or through other affiliated persons, material aid, assistance or advice on tax matters as a principal business or professional activity.

13a. persons other than those listed above who exercise a trust and company service provider activity in Luxembourg in a professional capacity;

14. providers of gambling services governed by the law of 20 April 1977 on gaming and betting on sporting events, as amended, acting in the course of their business;

14a. operators in a free zone authorised to exercise their activities pursuant to an authorisation by the *Administration des douanes et accises* within the Community control type 1 free zone located in the municipality of Niederanven Section B Senningen called Parishaff L-2315 Senningerberg (Hoehenhof).

15. other persons trading in goods, only to the extent that payments are made or received in cash in an amount of EUR 10,000 or more, whether the transactions or series of transactions are carried out in a single operation or in several operations which appear to be linked;

16. virtual asset service providers;

17. safekeeping or administration service providers;

18. 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;

19. persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more.

(2) The scope of application of this title and hence the concept of professional also includes branches in Luxembourg of foreign professionals as well as professionals established under the laws of foreign countries who supply services in Luxembourg without establishing any branch in Luxembourg.

Art. 2-1. Supervisory authorities and self-regulatory bodies

(1) The CSSF is the supervisory authority responsible for monitoring the compliance of credit institutions and, without prejudice to paragraph (3), the compliance of the professionals it supervises, licenses or registers, including branches of foreign professionals notified to the CSSF and professionals of foreign legal jurisdictions notified to the CSSF that provide services in Luxembourg without setting up branches, with their professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 5, and their implementing measures.

The CSSF is also the supervisory authority responsible for monitoring the compliance with the professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 5 and their implementing measures, of the tied agents, established in Luxembourg, of credit institutions or PSFs licensed or authorised to exercise their activities in Luxembourg pursuant to the law of 5 April 1993 on the financial sector, as amended, as well as of the Luxembourg-established agents of payment institutions and electronic money institutions licensed or authorised to exercise their activities in Luxembourg pursuant to the law of 10 November 2009 on payment services, as amended.

The CSSF is the supervisory authority responsible for monitoring the compliance with the professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 5 and their implementing measures, of foreign institutions for occupational retirement provision authorised to provide services to sponsoring undertakings in Luxembourg pursuant to the law of 13 July 2005 on the activities and supervision of institutions for occupational retirement provision, as amended.

(2) The CAA is the supervisory authority responsible for monitoring the compliance of the natural persons and legal persons referred to in Article 2 under its supervision, including that of branches of foreign professionals notified to the CAA, and that of professionals of foreign legal jurisdictions notified to the CAA that provide services in Luxembourg without setting up branches, with their professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 5 and their implementing measures.

(3) The *Institut des réviseurs d'entreprises* referred to in Title II, Part I of the law of 23 July 2016 on the audit profession shall ensure compliance by its members who are natural and legal persons referred to in point 8 of Article 2(1), as well as that of branches of audit professionals of foreign legal jurisdictions, and that of audit professionals of foreign legal jurisdictions that provide services in Luxembourg without setting up branches, with their professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 5 and their implementing measures.

(4) The *Ordre des experts-comptables* referred to in Title II of the law of 10 June 1999 on the organisation of the accounting profession, as amended, is responsible for monitoring the compliance of its natural person and legal person members referred to in point 9 of Article 2(1), as well as that of branches of professionals of foreign legal jurisdictions that exercise the activities referred to in Article 1(1) of the law of 10 June 1999 on the organisation of the accounting profession, as amended, and that of professionals of foreign legal jurisdictions that provide the services referred to in

Article 1(1) of the law of 10 June 1999 on the organisation of the accounting profession, as amended, in Luxembourg, without setting up branches, with their professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 5 and their implementing measures.

(5) The *Chambre des Notaires* referred to in Section VII of the law of 9 December 1976 on the organisation of the profession of notary, as amended shall ensure that the notaries referred to in point 11 Article 2(1) comply with their professional obligations as regards the fight against money laundering and terrorist financing provided for in Articles 2-2 to 5 and their implementing measures.

(6) The Luxembourg Bar Association is responsible for monitoring the compliance of the lawyers exercising the activities referred to in point 12 of Article 2(1) in Luxembourg with their professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 7 and their implementing measures.

By way of derogation from the first subparagraph, the Diekirch Bar Association is responsible for monitoring the compliance of its own members with their professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 7 and their implementing measures.

(7) The chamber of court bailiffs (*Chambre des huissiers*) referred to in Chapter VIII of the law of 4 December 1990 on the organisation of the service of court bailiffs, as amended ensures compliance by the bailiffs referred to in point (11a) of Article 2(1) of their professional obligations as regards the fight against money laundering and terrorist financing provided for in Articles 2-2 to 5 and their implementing measures.

(8) The AED is the supervisory authority responsible for monitoring the compliance of professionals not referred to in paragraphs (1) to (7) with their professional anti-money laundering and counter-terrorist financing obligations provided for in Articles 2-2 to 5 and their implementing measures.

Chapter 2: Professional obligations

Art. 2-2. Duty to carry out a risk assessment

(1) Professionals shall take appropriate measures to identify, assess and understand the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those measures shall be proportionate to the nature and size of the professionals.

(2) Professionals shall contemplate all relevant risk factors before determining the aggregate risk, and the type and stringency of measures appropriate to manage and mitigate the risks. In addition, professionals shall ensure that the risk information included in national and supranational risk assessments or communicated by supervisory authorities, self-regulatory bodies or European Supervisory Authorities are integrated in their risk assessments. Professionals shall be required to document, keep up-to-date and make available to supervisory authorities and self-regulatory bodies the risk assessments referred to in paragraph (1). Supervisory authorities and self-regulatory bodies may decide that individual documented risk assessments are

not required if the specific risks inherent in the sector are clearly identified and understood.

(3) Professionals shall identify and assess the risks of money laundering and terrorist financing that may result from the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies in connection with new or pre-existing products.

Professionals shall:

(a) assess risks before the launch or use of such products, practices and technologies; and

(b) take appropriate measures to manage and mitigate these risks.

Art. 3. Customer due diligence

(1) Professionals shall apply customer due diligence measures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out an occasional transaction:

(i) that 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) that constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, hereinafter "Regulation (EU) 2015/847", exceeding EUR 1,000;

(ba) 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;

(bb) for 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;

(c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

A Grand Ducal regulation may modify the thresholds laid down in this paragraph.

(2) Customer due diligence measures shall include:

(a) identifying the customer and verifying their identity, on the basis of documentation, data or information from reliable and independent sources including, where applicable, the relevant electronic identification means and trust services provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, hereinafter "Regulation (EU) 910/2014", or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;

(b) identifying the beneficial owner and taking reasonable measures to verify their identity using relevant information or data obtained from a reliable and independent source, in such a way that the professional is satisfied that it knows who the beneficial owner is - including, in the case of legal persons, *fiducies*, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer.

For legal person customers, professionals shall identify and take reasonable measures to verify the identity of beneficial owners by means of the following information:

(i) the identities of the natural persons, if any, who ultimately hold a controlling ownership in a legal person within the meaning of point (a)(i) of Article 1(7); and

(ii) after having applied point (i), to the extent that there is any doubt as to whether the persons holding a controlling ownership are the beneficial owners, or where no natural person holds such a controlling interest, the identities of any natural persons exercising control over the legal person by other means; and

(iii) where no natural person is identified by application of points (i) or (ii), the identity of any relevant natural person who holds the position of a senior managing official.

Professionals shall keep records of the measures taken and on any difficulties encountered during the verification process.

For customers that are legal arrangements, professionals shall identify the beneficial owners and take reasonable measures to verify the identity of these persons by means of the following information:

(i) in the case of *fiducies* and trusts, the identity of any settlors, *fiduciaires*, trustees, trust protectors or beneficiaries or, where the persons benefiting from the legal arrangement or entity have not yet been designated, the category of persons in whose main interest the legal arrangement or entity was primarily formed or primarily operates, and any other natural person exercising ultimate control of the *fiducie* or trust through direct or indirect ownership or by other means, including through a chain of ownership or control;

(ii) in the case of other legal arrangements similar to *fiducies* or trusts, the identity of persons holding equivalent or similar positions to those referred to in point (i);

(c) assessing and understanding the purpose and intended nature of the business relationship and, where necessary, obtaining information on the purpose and intended nature of the business relationship;

(d) performing ongoing monitoring of the business relationship – in particular, scrutiny of the transactions undertaken throughout the course of that relationship including, where necessary, of the source of funds – to ensure that the transactions are consistent with the professional's knowledge of the customer, the customer's business and its risk profile, while ensuring that the documents, data and information obtained in the customer due diligence process are kept up to date and relevant. To this purpose, professionals shall review all existing records, in particular for higher-risk categories of customers.

Where applicable, the identification and verification obligations provided for in points (a) and (b) of the first subparagraph shall also include:

(a) for all customers, an obligation to verify that any person purporting to act for or on behalf of the customer is authorised to do so, and to verify that person's identity;

(b) for customers that are legal persons or legal arrangements:

(i) an obligation to understand the nature of its activity as well as its ownership and control structure;

(ii) an obligation to verify the name, legal form and factual existence of the legal person or legal arrangement, in particular by obtaining proof of its incorporation, or equivalent proof of its establishment or existence as of the relevant time;

(iii) an obligation to obtain information on the customer's name, the names of directors of *fiducies*, the legal form, the address of the registered office and the address one of the primary business premises (if different), the names of the relevant persons holding the management positions of the legal person or legal arrangement, and the provisions governing the power to bind the legal person or legal arrangement.

In the case of a real estate transaction, the professionals referred to in points 10 and 10a of Article 2(1) shall apply customer due diligence measures in respect of both the acquirers and the sellers of the real estate.

(2a) Professionals shall apply each of the customer due diligence requirements laid down in paragraph (2). Professionals shall determine the scope of these measures on the basis of their assessment of the risks relating to particular types of customer, to countries or geographical regions, or to products, services, transactions or delivery channels. In all circumstances, professionals shall identify the client and beneficial owner as referred to in paragraph (2).

Professionals shall consider, in their assessment of the money laundering and terrorist financing risks relating to particular types of customer, particular countries or geographical regions, or particular products, services, transactions or delivery channels, the risk variables relating to these risk categories. These variables, accounted for individually or in combination, may increase or decrease the potential risk and, as a result, impact the appropriate level of due diligence measures to be applied. In particular, these variables include the variables listed in Annex II.

Professionals shall be able to demonstrate to supervisory authorities or self-regulatory bodies that the measures they apply in accordance with this Article, Articles 3-1, 3-2 and 3-3 and their implementing measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

Professionals shall not rely exclusively on central registers such as those referred to in Articles 30(3) and 31 (3a) of Directive (EU) 2015/849 to meet their customer due diligence requirements under this Article, Articles 3-1, 3-2 and 3-3 and their implementing measures. Professionals shall meet these requirements by applying a risk-based approach.

(2b) For life or other insurance business related to investments which they make or negotiate, in addition to the customer due diligence measures required for the customer and the beneficial owner, credit institutions and financial institutions 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 credit institutions or financial institutions that it will be able to establish the identity of the beneficiary at the time of the payout.

With regard to the preceding points (a) and (b), 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, credit institutions and financial institutions 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.

Credit institutions and financial institutions shall consider the beneficiary of a life insurance policy as a relevant risk factor when determining whether to apply enhanced due diligence measures. If a credit institution or a financial institution establishes that the beneficiary of a life insurance policy which is a legal person or legal arrangement presents a higher risk, enhanced due diligence measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary of the life insurance policy at the time of the payout. They shall make a suspicious transaction report to the FIU wherever the circumstances give rise to a suspicion of money laundering or terrorist financing.

(2c) In the case of beneficiaries of *fiducies*, of trusts or of similar legal arrangements that are designated by particular characteristics or category, the professionals shall obtain sufficient information concerning the beneficiary to ensure that they are able to identify the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

(…)[2]

(4) Verification of the identity of the customer and the beneficial owner shall take place before the establishment of a business relationship or the carrying out of the transaction. When building a new business relationship with a company or other legal person, a *fiducie*, a trust or a legal arrangement with a similar structure or similar roles to those of a trust for which information on the beneficial owners must be recorded pursuant to Article 30 or 31 of Directive (EU) 2015/849, professionals shall collect proof this record or a certificate from a registry.

However, the verification of the identity of the customer and the beneficial owner may be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations, these measures shall be taken as soon as possible after the initial contact and professionals shall take measures to effectively manage the risk of money laundering and terrorist financing.

Notwithstanding the first subparagraph of this paragraph, the opening of an account with a credit institution or financial institution, including accounts that permit transactions in transferable securities, is permitted on an exceptional basis where this is essential in order to prevent the disruption of normal business operations, and the risks of money laundering and terrorist financing are being effectively managed, provided that there are sufficient safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the customer due diligence requirements set out in points (a) and (b) of paragraph (2) is obtained and the measures necessary to achieve it are being implemented as soon as reasonably practicable. The keeping of anonymous accounts, anonymous passbooks or anonymous safe deposit boxes as well as accounts under patently fictitious names is prohibited.

Professionals which are unable to comply with points (a) to (c) of paragraph (2) and, where relevant, paragraphs (2b) and (2c) shall neither perform a transaction through a bank account, nor establish a business relationship, nor carry out a transaction, and must terminate the business relationship, and must consider making a suspicious transaction report to the FIU, in accordance with Article 5.

Subparagraph 4 is not applicable to professionals referred to in points 8, 9, 11, 11a, 12 and 13, letter (a) of Article 2(1) to the strict extent that those persons ascertain the legal position of their customer, or perform the task of defending or representing that customer in, or in relation to, judicial proceedings, including providing advice on instituting or avoiding such proceedings.

[2] Repealed by the law of 25 March 2020 – AML5.

Professionals shall also adopt risk management procedures regarding the conditions under which a customer can benefit from the business relationship before the verification of the identity.

Where a professional suspects that a transaction may relate to money laundering or terrorist financing and reasonably believes that performing its due diligence duties would result in the customer being alerted, it may choose not to proceed and may report a suspicious transaction to the FIU.

(5) Professionals are required to perform customer due diligence not only for all new customers, but also for existing customers as and when appropriate, based on their assessment of the risks taking account of any existing prior customer due diligence procedures and the time at which they were implemented, or whenever the factors relevant to a customer's situation change, or where, in the course of the calendar year in question, the professional has any legal obligation to contact the customer in order to review all relevant information with respect to the beneficial owner(s), or where the professional became subject to this obligation pursuant to the law of 18 December 2015 on the Common Reporting Standard (CRS), as amended.

(6) Professionals are required to retain and promptly provide the documents, data and information below for the purpose of preventing, detecting and investigating of possible money laundering or terrorist financing by the Luxembourg authorities responsible for the fight against money laundering and terrorist financing or by self-regulatory bodies:

(a) with respect to customer due diligence measures, copies or reference numbers of documents, data and information required for compliance with the customer due diligence obligations provided for in Articles 3 to 3-3, including, where applicable, data obtained using electronic means of identification, relevant trust services provided for in Regulation (EU) No 910/2014 or any other secure process of identification, whether electronic or remote, which is regulated, recognised, approved or permitted by the relevant national authorities, accounts, commercial correspondence, as well as the results of all analyses conducted for a period of five years after the end of the business relationship with the customer, or after the transaction date for occasional transactions;

(b) the supporting evidence and records of transactions required to identify or reconstruct individual transactions, in order to provide proof, if necessary, evidence in the context of a preliminary criminal enquiry or criminal investigation, for a period of five years after the end of the business relationship with the customer, or after the transaction date for occasional transactions.

The retention period referred to in this paragraph, including any extended retention period not to exceed five additional years, shall also apply with respect to data accessible through the centralised mechanism referred to in Article 32a of Directive (EU) 2015/849.

Professionals are also required to keep information on the measures taken to identify beneficial owners within the meaning of points (a)(i) and (ii) of Article 1(7).

Without prejudice to the longer retention periods prescribed by other laws, professionals shall delete the personal data at the end of the retention periods referred to in the first subparagraph.

The supervisory authorities may require, in specific cases, where necessary for the performance of their duties under this law, that a professional keep the data for an additional period not exceeding five years.

By way of derogation from subparagraph 4, professionals shall retain personal data for an additional period of five years where such retention is necessary for the efficient implementation of internal measures to prevent or detect acts of money laundering or terrorist financing.

(6a) The processing of personal data pursuant to this law is subject to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter "Regulation (EU) 2016/679".

Personal data shall only be processed on the basis of this law by professionals for the purpose of preventing money laundering and terrorist financing and shall not be further processed in a manner inconsistent with those purposes. The processing of personal data on the basis of this law for any other purpose is prohibited.

Professionals shall communicate the information required pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 to new customers before establishing a business relationship or carrying out an occasional transaction. This information shall in particular contain a general warning on the legal obligations of professionals under this law with regard to the processing of personal data for the purpose of preventing money laundering and terrorist financing.

Pursuant to Article 5(5), first subparagraph, data controllers shall restrict or defer the relevant person's exercise of its right of access to its personal data where this is both necessary and proportionate in order to:

(a) enable the professional, the Financial Intelligence Unit, a supervisory authority or a self-regulatory body to carry out its tasks as appropriate for the purposes of this law or its implementing measures; or

(b) avoid obstructing official or legal inquiries, analyses, investigations or formal or judicial proceedings for the purposes of this law, its implementing measures or Directive (EU) 2015/849 and in order not to jeopardise the prevention, detection or investigation of money laundering or terrorist financing.

Personal data processed on the basis of this law in order to prevent money laundering and terrorist financing is done on grounds of public interest under Regulation (EU) 2016/679.

(7) Professionals shall pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

Art. 3-1. Simplified customer due diligence

(1) Where professionals identify areas of lower risk of money laundering and terrorist financing, they may apply simplified customer due diligence measures.

(2) Before applying simplified customer due diligence measures, professionals shall ensure that the business relationship or the transaction presents a lower degree of risk.

When assessing the risks of money laundering and terrorist financing relating to certain types of customers, geographic areas, and particular products, services, transactions or delivery channels, professionals shall take into account at least the factors of potentially lower risk situations set out in Annex III.

Professionals carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

(3) Professionals are required to gather sufficient information in every circumstance to determine whether the customer satisfies all of the conditions required to apply the simplified customer due diligence measures, which means that professionals must have access to a reasonable amount of information relating to the requirements set forth in Article 3(2) and must monitor the business relationship at all times so as to ensure that the conditions for the application of Article 3-1 continue to be met.

(4) Notwithstanding points (a), (b) and (c) of Article 3(2) and Article 3(4), and without prejudice to paragraph (1) of this article, based on an appropriate risk assessment which demonstrates a low risk, professionals are permitted not to apply certain customer due diligence measures with respect to electronic money, where all of the following risk-mitigating conditions are met:

(a) the payment instrument is not reloadable, or has a maximum monthly payment transaction limit of EUR 150 which can be used only in Luxembourg;

(b) the maximum amount stored electronically does not exceed EUR 150;

(c) the payment instrument is used exclusively to purchase goods or services;

(d) the payment instrument cannot be funded with anonymous electronic money;

(e) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

The exception provided for in the first subparagraph does not apply to cash refunds or cash withdrawals of the monetary value of electronic money where the amount refunded exceeds EUR 50, or to remote payment transactions within the meaning of point (6) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, hereinafter “Directive (EU) 2015/2366”, where the amount paid exceeds EUR 50 per transaction.

When making acquisitions, credit institutions and financial institutions shall only accept payment by anonymous prepaid cards issued in third countries if such cards meet equivalent requirements to those listed in subparagraphs 1 and 2.

(5) If there is information available which gives reason to believe that the degree of risk is not lower, or where there is any suspicion of money laundering or terrorist financing, or where there is any doubt as to the truthfulness or relevance of data previously obtained, or in specific cases of higher risk, this regime of simplified customer due diligence cannot be applied to those particular customers, geographical regions, products, services, transactions or delivery channels.

(6) The scope and methods of application of this regime for simplified customer due diligence can be modified or extended to other customers, products or transactions not listed in this article by way of Grand Ducal regulation.

A Grand Ducal regulation can also restrict or to entirely prohibit the application of this regime for simplified customer due diligence relating the customers, products or transactions listed in this article, if this regime is not justified given the risk of money laundering or terrorist financing.

Art. 3-2. Enhanced customer due diligence

(1) Professionals are required to apply, on a risk-sensitive basis, enhanced customer due diligence measures, in addition to the measures referred to in Article 3, in situations which present a higher risk of money laundering or terrorist financing, and at least in the cases described in paragraphs (2), (3) and (4), in order to manage and mitigate those risks appropriately.

When assessing the risks of money laundering and terrorist financing, professionals shall take into account at least the factors of potentially higher-risk situations set out in Annex IV.

Enhanced customer due diligence measures need not be invoked automatically with respect to branches or majority-owned subsidiaries which are located in high-risk countries, where those branches or majority-owned subsidiaries fully comply with group-wide policies and procedures in accordance with Article 4-1 or Article 45 of Directive (EU) 2015/849. Professionals shall handle these situations by using a risk-based approach.

Professionals are required to 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 unusual pattern;

(d) they do not have an apparent economic purpose or apparent lawful purpose.

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

(2) With respect to business relationships or transactions involving high-risk countries, professionals shall apply the following enhanced customer due diligence measures:

(a) obtaining additional information on the customer and on the beneficial owner(s), and more frequently updating customer and beneficial owner identification data;

(b) obtaining additional information on the intended nature of the business relationship;

(c) obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner(s);

(d) obtaining information on the reasons for the intended or performed transactions;

(e) obtaining the approval of senior management for establishing or continuing the business relationship;

(f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Professionals shall ensure, where applicable, that the first payment be carried out through an account in the customer's name with a credit institution subject to customer due diligence standards that are not less robust than those laid down in Directive (EU) 2015/849.

(2a) In addition to the measures provided in paragraph (2) and in compliance with the European Union's international obligations, supervisory authorities and self-regulatory bodies shall require professionals to apply, where applicable, one or more additional mitigating measures to persons and legal entities carrying out transactions involving high-risk countries.

Those measures shall consist of one or more of the following:

(a) the application of additional elements of enhanced due diligence;

(b) the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;

(c) the limitation of business relationships or transactions with natural persons or legal entities from high-risk countries.

(2b) In addition to the measures provided in paragraph (2), supervisory authorities and self-regulatory bodies shall apply, where applicable, one or several of the following measures with regard to high-risk countries, in compliance with the European Union's international obligations:

(a) refusing the establishment of subsidiaries or branches or representative offices of professionals from the country concerned, or otherwise taking into account the fact that the relevant professional is from a country that does not have adequate anti-money laundering and counter-terrorist financing regimes;

(b) prohibiting professionals from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate anti-money laundering and counter-terrorist financing regimes;

(c) requiring increased supervisory examination or increased external audit requirements for branches and subsidiaries of professionals located in the country concerned;

(d) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned;

(e) requiring credit and financial institutions to review and amend, or if necessary terminate, correspondent relationships with respondent institutions in the country concerned.

(2c) When enacting or applying the measures set out in paragraphs (2a) and (2b), supervisory authorities and, where applicable, self-regulatory bodies shall take into account, as appropriate, relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, in relation to the risks posed by individual countries.

(2d) Supervisory authorities or, where applicable, self-regulatory bodies shall notify the European Commission before enacting or applying the measures set out in paragraphs (2a) and (2b).

(3) In the case of cross-border correspondent relationships and other similar relationships with respondent institutions, when establishing the business relationship, credit institutions, financial institutions and other institutions concerned by those relationships shall, in addition to the customer due diligence measures laid down in Article 3(2):

(a) gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision which entails, in particular, finding out whether the institution was the subject of an investigation or other measures by a supervisory authority in the fight against money laundering and terrorist financing;

(b) assess the anti-money laundering and counter-terrorist financing control measures in place at the respondent institution;

(c) obtain approval at a senior level of management before establishing new correspondent relationships;

(d) clearly understand and document the respective responsibilities of each institution relating to the fight against money laundering and terrorist financing;

(e) with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of and performed ongoing due diligence on customers having direct access to accounts of credit institutions, financial institutions and other institutions concerned by these relationships, and be satisfied that it can provide relevant customer due diligence data and information to the correspondent institution upon request.

It is prohibited for professionals to enter into or continue a correspondent relationship with a shell bank, or with a credit institution or financial institution that is known to enable its accounts to be used by a shell bank. Professionals shall ensure that their correspondents do not authorise shell banks to use their accounts.

(4) With respect to transactions or business relationships with politically exposed persons, professionals shall, in addition to the customer due diligence measures provided for in Article 3:

(a) have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or beneficial owner is a politically exposed person;

(b) obtain approval at a senior level of management before establishing – or, with respect to existing customers, before continuing – a business relationship with such persons. In addition, credit institutions and financial institutions shall take all appropriate measures to establish the source of wealth and source of funds of the customers and beneficial owners identified as being politically exposed persons;

(c) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;

(d) conduct enhanced ongoing monitoring of those business relationships.

The provisions of this paragraph also apply where a customer has already been accepted and the customer or the beneficial owner is subsequently found to be, or subsequently becomes, a politically exposed person.

Professionals shall take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy or, where required, the beneficial owner of the beneficiary are politically exposed persons.

Those measures shall be taken no later than 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 3, professionals shall:

(a) inform senior management before payout of policy proceeds;

(b) conduct enhanced scrutiny of the entire business relationship with the policyholder; and

(c) make a suspicious transaction report to the FIU or, if the professional is a lawyer, to the president of the appropriate bar association, if the circumstances give rise to suspicions of money laundering or terrorist financing.

Where a natural person who holds or has been entrusted with a significant public function is no longer entrusted with a significant public function by a Member State or a third country, or with a prominent public function by an international organisation, professionals shall, for at least twelve months, be required to take into account the continuing risk posed by that politically exposed person and to apply appropriate and risk-sensitive measures, until such time as that person no longer poses any particular risk.

(…)[3]

(6) Professionals shall pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

(7) The mandatory application and the modalities of application of enhanced customer due diligence can be modified, supplemented or extended to other situations representing a high risk of money laundering or terrorist financing by a Grand Ducal regulation.

Art. 3-3. Performance of customer due diligence by third parties

(1) For the purposes of this article, "third parties" means: professionals listed in Article 2, the member organisations or federations of those professionals, or other institutions or persons situated in a Member State or third country that:

(a) apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this law or Directive (EU) 2015/849; and

(b) are subject, regarding compliance with the requirements of this law, of Directive (EU) 2015/849 or equivalent rules applicable to them, to supervision consistent with Chapter VI, Section 2 of Directive (EU) 2015/849.

Professionals are prohibited from relying on third parties established in high-risk countries. Third parties which are branches or majority-owned subsidiaries of professionals established in the European Union are exempt from this prohibition, provided these branches and majority-owned subsidiaries fully comply with their group-wide policies and procedures, in accordance with Article 4-1 or Article 45 of Directive (EU) 2015/849.

(2) Professionals may rely on third parties in order to meet the obligations provided for in Article 3(2) first subparagraph, points (a) to (c) and in the second subparagraph, if it has been ensured that the third party they rely on will be able to immediately obtain the information referred to in paragraph 3. However, the ultimate responsibility for

[3] Repealed by the law of *25 March 2020 – AML*.

meeting those requirements shall remain with the professionals which rely on the third party.

Professionals which rely on third parties must take appropriate measures to ensure that those third parties will provide, upon request and without delay, in accordance with paragraph (3), the necessary documents concerning the customer due diligence obligations provided for in Article 3(2), first subparagraph, points (a) to (c) and in the second subparagraph, including, where applicable, data obtained through the use of electronic identification means, the relevant trust services provided for in Regulation (EU) No 910/2014, or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities.

Professionals which rely on third parties must also satisfy themselves that the third party in question is regulated, subject to supervision, and that it has implemented measures to comply with the customer due diligence obligation the record-keeping requirements, which are in line with those provided for in Articles 3 to 3-2 of this law.

(3) Where a third party acts in accordance with paragraph (2) above, it shall, in accordance with the requirements set out in Article 3(2) first subparagraph, points (a) to (c) and in the second subparagraph and notwithstanding any applicable rules on confidentiality or professional secrecy, make the information requested immediately available to the professional to whom the customer is being referred. In such a case, relevant copies of identification and verification data including, where applicable, data obtained through the use of electronic identification means, the relevant trust services provided for in Regulation (EU) No 910/2014, or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities, and of any other relevant documentation on the identity of the customer or the beneficial owner shall immediately be forwarded, on request, by the third party to the professional to which the customer is being referred.

(4) The requirements set out in paragraphs (1) and (3) are considered to be met by professionals in their group programme when the following conditions are met:

(a) professionals rely on information provided by a third party belonging to the same group;

(b) this group applies customer due diligence measures, rules on the retention of documents and anti-money laundering, and anti-terrorist financing programmes in accordance with this law, Directive (EU) 2015/849 or equivalent rules;

(c) the effective implementation of the requirements referred to in point (b) is be monitored at group level by a supervisory authority, a self-regulatory body or one of their foreign counterparts;

(d) any risk relating to a high-risk country has been satisfactorily mitigated in accordance with Article 4-1(3) and (4).

(5) This article 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 professional covered by this law.

(6) A Grand Ducal regulation can restrict or entirely prohibit the option of relying on third parties or certain third parties, if this option is not justified given the risk of money laundering or terrorist financing.

Art. 4. Adequate internal management requirements

(1) Professionals shall put in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified at international, European, national and sectoral level and at the level of the professional. These policies, controls and procedures, which take into account the risks of money laundering and terrorist financing, shall be proportionate to the nature, specificities and size of the professionals.

The policies, controls and procedures referred to in the first subparagraph shall include:

(a) the development of internal policies, controls and procedures, including risk management models, customer due diligence, cooperation, record keeping, internal controls, risk assessment, risk management and compliance management, including the appointment, at the appropriate level of management, of a compliance officer (*responsable du contrôle du respect des obligations*) and the selection of staff;

(b) where appropriate with regard to the size and nature of the business and to the risks of money laundering and terrorist financing, an independent audit function to test the internal policies, controls and procedures referred to in point (a).

Professionals shall obtain approval from their senior management for the policies, controls and procedures that they put in place and shall monitor and enhance the measures taken, where appropriate.

Professionals shall, where applicable, appoint from among the members of their management body or their effective management the person responsible for compliance with professional obligations as regards the fight against money laundering and terrorist financing.

The internal control mechanism, including the internal audit function, shall be adequately resourced to test compliance, including sample testing, with the procedures, policies and control measures, and it shall enjoy sufficient autonomy to perform its duties. The compliance officer (*responsable du contrôle du respect des obligations*) and other members of staff involved shall have timely access to customer identification data and other information stemming from due diligence measures, transaction records and other relevant information. The compliance officer (*responsable du contrôle du respect des obligations*) shall be able to act independently and to make reports to the management without the need to consult their direct supervisor, or to the board of directors.

An adequate internal organisational structure shall include appropriate procedures to be followed when hiring new employees, so as to ensure that the hiring process relies on applicable professional repute, competence and experience criteria.

(2) Professionals shall take measures proportionate to their risks, nature and size so that their employees, including the members of their management bodies or their *de facto* management, are aware of the professional obligations as regards the fight against money laundering and terrorist financing, as well as the applicable data protection requirements. Those measures shall include participation of their employees in special continuing vocational training programmes designed to keep employees informed of new developments, including information on techniques, methods and trends in money laundering and terrorist financing; to help them recognise transactions which may be related to money laundering or terrorist financing; and to instruct them as to how to proceed in such cases. The special continuing vocational training programmes shall give employees clear explanations of all aspects of the law and anti-money laundering and counter-terrorist financing requirements, in particular of the obligations related to customer due diligence and the reporting of suspicious transactions.

Where a natural person falling within any of the categories listed in Article 2(1) exercises professional activities as an employee of a legal person, the obligations in this section shall apply to that legal person rather than to the natural person.

(2a) Supervisory authorities, self-regulatory bodies and the Financial Intelligence Unit shall ensure that professionals have access to up-to-date information on the practices of criminals who commit money laundering or terrorist financing offences and on indications that enable suspicious transactions to be identified.

(3) Professionals shall have systems in place that enable them to respond fully and rapidly to enquiries from the Luxembourg authorities responsible for combating money laundering and terrorist financing and from self-regulatory bodies as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship, through secure channels and in a way that guarantees the total confidentiality of requests for information.

(4) Professionals shall have in place appropriate policies proportionate to their risks, nature and size enabling their employees or persons in a comparable situation to report internally breaches of professional obligations as regards the fight against money laundering and terrorist financing through a specific, independent and anonymous channel.

Art. 4-1. Group-wide policies and procedures

(1) Professionals 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 as regards the fight against money laundering and terrorist financing. These policies and procedures shall be implemented effectively and in a suitably tailored manner, accounting in particular for the identified risks of money laundering and terrorist financing and for the nature, specificities, size and business of the branches and subsidiaries, at the level of the branches and majority-owned subsidiaries established in Member States and third countries.

Group-wide policies and procedures shall include:

(a) the policies, controls and procedures provided for in Article 4(1) and (2);

(b) making available, under the conditions in Article 5(5) and (6), information stemming from branches and subsidiaries about customers, accounts and transactions as and where required, for the purposes of the fight against money laundering and terrorist financing, by the compliance and audit functions, as well as for the fight against money laundering and terrorist financing at group level. In particular, this means data and analyses of transactions or activities that seem unusual, where such analyses have been conducted. This information may include information related to suspicious submissions or the reporting of such submissions to the FIU. By the same token, where relevant and appropriate for the purposes of risk management, branches and subsidiaries shall also receive this information from the group's compliance departments; and

(c) adequate safeguards with respect to confidentiality and the use of the information being exchanged, including safeguards to prevent disclosure of information.

(2) The professionals that operate establishments in another Member State shall ensure that these establishments comply with the domestic provisions implementing Directive (EU) 2015/849 within that other Member State.

(3) Professionals are required to apply measures at least equivalent to those provided for in Articles 2-2 to 7, in Directive (EU) 2015/849 or through the implementing measures with respect to risk assessment, customer due diligence, record keeping, appropriate internal organisation and cooperation with the authorities in their branches and majority-owned subsidiaries situated abroad.

In particular, professionals shall ensure that this principle is respected for branches and subsidiaries in high-risk countries. Where the minimum standards as regards the fight against money laundering and terrorist financing in a country in which a professional has branches and majority-owned subsidiaries are different to those applicable in Luxembourg, those branches and subsidiaries must apply the most stringent standard, insofar as the laws and regulations of the host country so permit. In this context, if the standards of the country in which these branches and subsidiaries are situated are less stringent than those in Luxembourg, the data protection rules applicable in Luxembourg relating to the fight against money laundering and terrorist financing must be complied with, insofar as the laws and regulations of the host country so permit.

(4) Where the law of a country does not permit the implementation of the policies and procedures required under paragraphs (1) and (3), professionals shall ensure that their branches and majority-owned subsidiaries in that third country apply additional measures to effectively handle the risk of money laundering or terrorist financing, and inform the supervisory authorities and self-regulatory bodies. If the additional measures are not sufficient, the supervisory authorities and the self-regulatory bodies 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 third country.

Art. 5. Cooperation requirements with the FIU, the authorities and self-regulatory bodies

(1) Professionals, their directors (*dirigeants*) and employees are obliged to cooperate fully with the Luxembourg authorities responsible for combating money laundering and terrorist financing and with self-regulatory bodies, in particular when they exercise their respective supervisory powers by virtue of Articles 8-2 and 8-2a. Without prejudice to the obligations *vis-à-vis* supervisory authorities or self-regulatory bodies, professionals, their directors (*dirigeants*) and employees are required to:

(a) inform without delay, on their own initiative, the Financial Intelligence Unit when they know, suspect or have reasonable grounds to suspect that money laundering, an associated underlying offence or terrorist financing is being committed or has been committed or attempted, in particular in consideration of the person involved, its development, the origin of the funds, or the nature, purpose or procedure of the operation. This report must be accompanied by all supporting information and documents having prompted the report.

All suspicious transactions, including attempts to perform suspicious transactions, must be reported, irrespective of their amount.

The obligation to report suspicious transactions shall apply regardless of whether those filing the report can determine the predicate offence.

(b) provide without delay to the Financial Intelligence Unit, at its request, any information required. This obligation includes the submission of the documents on which the information is based.

The identity of professionals, directors (*dirigeants*) and employees having provided such information is kept confidential by the aforementioned authorities, unless disclosure is essential to ensure the regularity of legal proceedings or to establish proof of the facts forming the basis of these proceedings.

(1a) With regard to combating terrorist financing, the obligation to report suspicious transactions set forth in paragraph (1), point (a) also applies to funds where there are reasonable grounds to suspect that they are, or where they are suspected to be, linked or related to, or used for, terrorism, terrorist acts, one or more terrorist groups or those who finance terrorism.

(2) The communication of information and documents referred to in paragraphs (1) and (1a) is usually carried out by the individual(s) appointed by the professionals for this purpose, in accordance with the procedures laid down in Article 4(1). The elements of information and documents provided to the authorities, other than the judicial authorities, pursuant to paragraphs (1) and (1a) may only be used in the combat against money laundering and terrorist financing.

(3) Professionals must refrain from carrying out any transaction which they know, suspect or have reasonable grounds to suspect to be related to money laundering, an associated underlying offence or terrorist financing before having informed the Financial Intelligence Unit thereof in accordance with paragraphs (1) and (1a) and having complied with any special instructions from the Financial Intelligence Unit. The Financial Intelligence Unit can give instructions not to execute operations relating to the transaction or the customer.

Where to refrain from a transaction falling under paragraph (1) is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected transaction, the professionals concerned shall inform the Financial Intelligence Unit without delay.

If instructions are given verbally, they shall be confirmed in writing within three business days. If no written confirmation is made, the instruction shall cease to have effect on the third business day at midnight.

The professional is not authorised to disclose this instruction to the customer without the express prior consent of the Financial Intelligence Unit.

At any time and at its own discretion, the Financial Intelligence Unit may give instructions to partially or fully revoke an order not to execute transactions in accordance with paragraph (1).

(3a) The provisions of paragraph (1)(b) and paragraph (3) apply even in the absence of a suspicious transaction report made by the professional in accordance with paragraph (1)(a) and paragraph (1a).

(4) No professional secrecy applies with regard to the Financial Intelligence Unit in respect of the provisions of paragraphs (1), (1a) and (3).

The disclosure in good faith to the Luxembourg authorities responsible for combating money laundering and terrorist financing to self-regulatory bodies or, if the professional is a lawyer, to the President of the respective bar association (*bâtonnier de l'Ordre des avocats*) by a professional or employee or a director (*dirigeant*) of such a professional of any information referred to above according to this article and Article 7 does not constitute a breach of any restriction on disclosure of information imposed by contract, by professional secrecy or by a legislative, regulatory or administrative provision and does not give rise to liability of any kind for the professional or the person concerned, even in a situation where they did not have precise knowledge of the associated underlying offence, irrespective of whether an unlawful activity actually took place.

Persons, including a professional's employees and representatives, shall not be subject to threats, retaliatory measures or hostile acts, and particularly adverse or discriminatory measures with respect to employment, for having reported suspicions of money laundering or terrorist financing to the FIU.

Persons who are exposed to threats, retaliatory measures, hostile acts, or adverse or discriminatory measures with respect to employment for having reported suspicions of money laundering or terrorist financing to the FIU shall have the right to file a complaint with the supervisory authority or self-regulatory body referred to in Article 2-1.

Any contractual provision or act that runs contrary to subparagraph 3, and in particular any termination of an employment contract in violation of subparagraph 3, is null and void by operation of law (*ipso jure*).

If an employee's employment contract is thus terminated, the employee may make recourse as provided for in Article L. 271-1 (4) to (7) of the Labour Code.

(4a) Reports, information and documents supplied by a professional pursuant to the provisions of paragraphs (1) and (1a) cannot be used against this professional in proceedings on the basis of Article 9.

(5) The professionals and their directors (*dirigeants*) and employees shall not disclose to the customer concerned or to other third persons the fact that information is, will be or has been reported or provided to the authorities pursuant to paragraphs (1), (1a), (2) and (3) or that a money laundering or terrorist financing investigation by the Financial Intelligence Unit is being or may be carried out.

This prohibition does not apply to a disclosure to the supervisory authorities or, if appropriate, the self-regulatory bodies of the different professionals.

The prohibition laid down in the first subparagraph shall not apply to disclosure between the credit and financial institutions of Member States where these belong to the same group, or between such institutions and their majority-owned branches and subsidiaries situated in third countries, provided that such majority-owned branches and subsidiaries fully comply with the policies and procedures defined at the level of the group, including the procedures as regards the sharing of information within the group, in accordance with Article 4-1 or Article 45 of Directive (EU) 2015/849, and that the policies and procedures defined at the level of the group comply with the requirements of this law or of Directive (EU) 2015/849.

The prohibition laid down in the first subparagraph shall not prevent the disclosure between professionals referred to in points 8, 9, 11, 12 and 13 of Article 2(1), situated in Member States or in Third Countries which impose requirements equivalent to those laid down in this law or in Directive (EU) 2015/849, who exercise their professional activities, whether as employees or not, within the same legal person or a network. For the purposes of this subparagraph, a “network” means the larger structure to which the person belongs and which shares common ownership, management and compliance control.

For credit institutions, financial institutions and professionals referred to in points 8, 9, 11, 12 and 13 of Article 2(1), in cases related to the same person and the same transaction involving two or more professionals, the prohibition laid down in the first subparagraph of this paragraph shall not prevent disclosure between the relevant professionals provided that they are situated in a Member State, or in a Third Country which imposes requirements equivalent to those laid down in this law or in Directive (EU) 2015/849 and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged must be used exclusively for the purposes of the prevention of money laundering and terrorist financing.

By way of derogation from the preceding subparagraphs, a Grand Ducal regulation can prohibit the disclosure between the aforementioned professionals and institutions or persons situated in a third country if there is a risk of money laundering or terrorist financing.

Where the professionals referred to in points 8, 9, 11, 12 and 13 of Article 2(1), seek to dissuade a customer from engaging in illegal activity, this shall not constitute a disclosure within the meaning of the first subparagraph.

(6) Information concerning suspicions that funds are derived from money laundering or an associated underlying offence or relate to terrorist financing which has been reported to the FIU shall be shared within the group, unless the FIU instructs otherwise.

Chapter 3: Specific provisions for certain professionals

Section 1: Specific provisions applicable to the insurance sector

Art. 6. Repealed[4]

Section 2: Specific provisions applicable to lawyers

Art. 7.

(1) Lawyers are not subject to the obligations referred to in Article 3(4) subparagraph 5 and in Article 5(1) and (1a) with regard to information they receive from or obtain on one of their clients, in the course of providing legal advice or ascertaining the legal position for their client or performing the task of defending or representing that client in judicial proceedings or concerning such proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

(2) In lieu and instead of a direct information or transmission of documents to the Financial Intelligence Unit the information or documents referred to in Article 5(1) and (1a) have to be disclosed to the president of the bar association (*bâtonnier de l'Ordre des avocats*) on whose table the disclosing lawyer is registered in conformity with the law of 10 August 1991 on the legal profession, as amended. In this case, the president of the bar association (*bâtonnier de l'Ordre des avocats*) shall verify compliance with the conditions set out in the previous paragraph and in point 12 of Article 2. In case of compliance, he shall transmit the information or documents received to the Financial Intelligence Unit.

(3) By way of derogation from Article 3(6), subparagraph 6, a lawyer who suspects that a transaction relates to money laundering or terrorist financing and who reasonably believes that in fulfilling his customer due diligence duties, he would alert the customer, may choose not to proceed and may report a suspicious transaction to the president of the bar association on whose table he is registered. In this case, the president of the bar association (*bâtonnier de l'Ordre des avocats*) shall verify compliance with the conditions set out in the previous paragraph and in point 12 of Article 2(1). If this is confirmed, he shall be required to transmit the suspicious transaction report to the FIU.

Section 3: Specific provisions applicable to virtual asset service providers

Art. 7-1.

(1) Without prejudice to Article 4 of the law of 10 November 2009 on payment services, as amended, this article shall apply to providers of virtual asset services who exercise

[4] Law of 17 July 2008.

activities other than the provision of payment services of the type referred to in point 38 of Article 1 of this law. This shall apply to virtual asset service providers that are established or that provide services in Luxembourg.

(2) The virtual asset service providers referred to in paragraph (1) must be registered within the register of virtual asset service providers established by the CSSF. They shall submit an application form for registration to the CSSF, which shall include the following information:

(a) for natural person applicants:

(i) the applicant's last name and the first name(s);

(ii) the precise private address or the precise professional address, including:

- for addresses in the Grand Duchy of Luxembourg, the usual place of residence listed in the national register of natural persons; for professional addresses, the town, street name and building number listed in the national register of towns and street names, as provided for in Article 2(g) of the law of 25 July 2002 on the reorganisation of the Land Registry and Topography Administration (*Administration du cadastre et de la topographie*), as amended, and the postal code;

- for foreign addresses, the town, street name and building number in the foreign country, the postal code and the country name;

(iii) for persons registered in the national register of natural persons, the identification number provided for by the law of 19 June 2013 on the identification of natural persons, as amended;

(iv) for non-resident persons who are not registered in the national register of natural persons, a foreign national identification number;

(v) the service(s) corresponding to one or more of the services referred to in Article 1(20c);

(vi) a description of the risks of money laundering and terrorist financing to which the applicant will be exposed, and the internal control mechanisms established by the applicant to mitigate these risks and comply with the professional obligations defined in this law and in Regulation (EU) 2015/847, or in their implementing measures;

(b) for legal person applicants:

(i) the name of the applicant;

(ii) the applicant's precise central administrative address;

(iii) a description of the activities exercised including, in particular, a list of the intended types of virtual asset service and the applicant's corresponding qualifications;

(vi) a description of the risks of money laundering and terrorist financing to which the applicant will be exposed, and the internal control mechanisms established by the applicant to mitigate these risks and comply with the professional obligations defined in this law and in Regulation (EU) 2015/847, or in their implementing measures.

The CSSF shall keep and update the register referred to in the first subparagraph of this section and shall publish it on its website.

(3) Registration shall be subject to the condition that the persons who hold a management function in the entities referred to in paragraph (1) and the beneficial owners of such entities submit the necessary information to the CSSF to prove their professional repute.

Professional repute is assessed on the basis of criminal records and any other information that may be used to establish whether the persons referred to in the first subparagraph are of good repute and offer every guarantee of irreproachable business conduct.

At least two persons must be responsible for the management of the virtual asset service provider, and entitled to effectively determine the policy of the business activity. They shall have adequate professional experience.

Any change regarding the persons referred to in the first to third subparagraphs must be notified to the CSSF and approved by the CSSF beforehand. The CSSF will object to the intended change if the relevant persons do not have adequate professional repute or, where applicable, adequate professional experience.

The CSSF may request any information on persons subject to legal requirements with respect to professional repute or professional experience.

(3a) For natural persons, registration shall be subject to the condition that persons exercising a virtual asset service provider activity submit the necessary information to the CSSF to prove their professional repute and adequate professional experience.

Professional repute is assessed on the basis of criminal records and any other information that may be used to establish whether the persons referred to in the first subparagraph are of good repute and offer every guarantee of irreproachable business conduct.

The CSSF may request any information on persons subject to legal requirements with respect to professional repute or professional experience.

(4) Where the conditions in paragraph (3) fail to be met or the virtual asset service providers referred to in this article do not meet the requirements set out in Articles 2-2, 3, 3-1, 3-2, 3-3, 4, 4-1, 5 and 8-3 paragraph (3), the CSSF may remove the virtual asset service providers from the register referred to in paragraph (2).

(5) Any decision taken by the CSSF in accordance with this article may be brought before the competent administrative court (*tribunal administratif qui statue comme juge du fond*) within one month, after which period it shall be time-barred.

(6) The fact that a virtual asset service provider is listed in the register referred to in paragraph (2) shall under no circumstances, and in no way whatsoever, be construed as a positive assessment on the part of the CSSF of the quality of the services offered.

Section 4: Specific provisions applicable to trust and company service providers

Art. 7-2.

(1) Trust and company service providers shall register with the competent supervisory authority or self-regulatory body pursuant to Article 2-1. Applications for registration shall include the following information:

(a) for natural person applicants:

(i) the last name and the first name(s);

(ii) the precise private address or the precise professional address, including:

- for addresses in the Grand Duchy of Luxembourg, the usual place of residence listed in the national register of natural persons; for professional addresses, the town, street name and building number listed in the national register of towns and street names, as provided for in Article 2(g) of the law of 25 July 2002 on the reorganisation of the Land Registry and Topography Administration (*Administration du cadastre et de la topographie*), as amended, and the postal code;

- for foreign addresses, the town, street name and building number in the foreign country, the postal code and the country name;

(iii) for persons registered in the national register of natural persons, the identification number provided for by the law of 19 June 2013 on the identification of natural persons, as amended;

(iv) for non-resident persons who are not registered in the national register of natural persons, a foreign national identification number;

(v) the service(s) corresponding to one or more of the services referred to in Article 1(8).

(b) for legal person applicants:

(i) the corporate name of the legal person and, where applicable, the customary abbreviation and the trading name;

(ii) the precise address of the legal person's registered office;

(iii) if the applicant is

- a legal person registered in the Luxembourg trade and companies register, the registration number;

- a legal person not registered in the Luxembourg trade and companies register, where applicable, the name of the register where the legal person is registered, and its registration number if one is required under the law of the relevant country;

(iv) the service(s) corresponding to one or more of the services referred to in Article 1(8).

(2) The supervisory authorities may exempt trust and company service providers under their prudential supervision from the obligations referred to in paragraph (1) where they are already licensed or authorised to act as trust and company service providers.

(3) Supervisory authorities and self-regulatory bodies shall coordinate in order to establish and maintain an up-to-date list of the trust and company service providers under their jurisdiction pursuant to Article 2-1.

This list shall indicate, for each trust and company service provider, the relevant supervisory authority or self-regulatory body as well as any exemption granted pursuant to paragraph (2).

(4) With respect to trust and company service providers subject to the supervisory powers of a self-regulatory body, the obligations in paragraph (1) are considered professional obligations flowing from the legislation on the fight against money laundering and terrorist financing within the meaning of point (1a) of Articles 71 and 100-1 of the law of 9 December 1976 on the organisation of the profession of notary, as amended; point (4) of Articles 32 and 46-1 of the law of 4 December 1990 on the organisation of the service of court bailiffs, as amended; Article 17, point 6 of Article 19 and Article 30-1 of the law of 10 August 1991 on the legal profession, as amended; Articles 11(f) and 38-1 of the law of 10 June 1999 on the organisation of the accounting profession, as amended and Articles 62(d) and 78(1)(c) of the law of 23 July 2016 on the audit profession, as amended.

(5) For natural persons subject to the supervision of the AED pursuant to Article 2-1 (8) and exercising trust and company service provider activities, registration shall be subject to the condition that these natural persons have adequate professional repute and submit the necessary information to prove this to the AED.

For legal entities subject to the supervision of the AED pursuant to Article 2-1(8) and exercising trust and company service provider activities, registration shall be subject to the condition that the persons who hold a management function within those legal entities and the beneficial owners of those legal entities have adequate professional repute and submit the necessary information to prove this to the AED.

Professional repute is assessed on the basis of criminal records and any other information that may be used to establish whether the persons referred to in the first and second subparagraphs are of good repute and offer every guarantee of irreproachable business conduct.

Any change regarding the persons referred to in the second subparagraph shall be notified to the AED.

The AED may request any information on persons subject to legal requirements with respect to professional repute.

All trust and company service providers subject to the supervision of the AED pursuant to Article 2-1 (8) that cease their activities shall notify the AED of this.

Chapter 3-1: Supervision and sanctions

Section 1 – Supervision of professionals

Art. 8-1. Exercise of supervisory powers by supervisory authorities and self-regulatory bodies

(1) The supervisory authorities and self-regulatory bodies effectively supervise compliance by professionals with their professional obligations in the fight against money laundering and terrorist financing and take the necessary measures in this respect.

(1a) Supervisory authorities and self-regulatory bodies shall provide professionals with information on countries that do not apply, or apply insufficient, measures to combat money laundering and terrorist financing, and in particular about the concerns raised by the weaknesses in those countries' mechanisms for fighting money laundering and terrorist financing.

Supervisory authorities can require credit institutions and financial institutions to adopt one or more enhanced due diligence measures which are proportionate to the risks listed in Article 3-2(2) to (2c) when conducting business relationships and transactions with natural persons or legal entities involving such countries.

(2) Where a professional that has its registered office in another Member State operates establishments in Luxembourg, the supervisory authorities and self-regulatory bodies shall monitor the compliance of the establishments operated in Luxembourg with the obligations provided for in Articles 2-2, 3, 3-1, 3-2, 3-3, 4, 4-1, 5, 7 and 8-3(3), or in their implementing measures.

The supervisory authorities and self-regulatory bodies shall cooperate with their respective counterparts in the Member State in which the registered office of the professional is located in order to ensure effective supervision of compliance with the provisions of this law, its implementing measures and Directive (EU) 2015/849.

In the case of credit institutions and persons referred to in Article 1(3a) letters (a) to (e) and (g) which are established in other Member States that are part of a group whose parent company is established in Luxembourg, the CSSF and the CAA shall cooperate with their respective counterparts in the Member States in which the institutions forming part of the group are established in order to ensure that these institutions comply with the Member State's domestic provisions implementing Directive (EU) 2015/849.

In the cases referred to in subparagraph 3, the CSSF and the CAA shall supervise the effective implementation of group-wide policies and procedures referred to in Article 4-1(1).

In the case of credit institutions and persons referred to in Article 1(3) letters (a) to (e) and (g) which are established in Luxembourg and which belong to a group whose parent company is established in another Member State, the CSSF and the CAA shall cooperate with their respective counterparts in the Member State in which the parent company is established in order to monitor the effective implementation of group-wide policies and procedures referred to in Article 45(1) of Directive (EU) 2015/849.

(3) In the case of issuers of electronic money within the meaning of point (3) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (hereinafter "Directive 2009/110/EC"), and of payment service providers within the meaning of point (11) of Article 4 of Directive (EU) 2015/2366, which are established in Luxembourg in a form other than a branch and whose registered office is situated in another Member State, supervision referred to in paragraph (2), first subparagraph, may include the adoption of appropriate and proportionate measures on the basis of Article 8-4 in order to remedy serious breaches requiring immediate intervention. Such measures shall be temporary and shall cease when the identified breaches have been remedied, including with the assistance of, or in cooperation with, the supervisory authorities of the Member State in which the professional has its registered office. Issuers of electronic money within the meaning of point (3) of Article 2 of Directive 2009/110/EC and payment service providers within the meaning of point (11) of Article 4 of Directive 2007/2015/EC which are established in Luxembourg in a form other than a branch, which have their registered office in another Member State and which meet at least one of the criteria provided for in the implementing measures for Article 45(9) of Directive (EU) 2015/849 shall appoint a central contact point in Luxembourg to ensure, on behalf of the appointing institution, compliance with anti-money laundering and counter-terrorist financing rules, and to facilitate the supervision conducted by the CSSF. The central contact point in Luxembourg shall provide to the CSSF, upon its request, all documents and information needed for it to perform its duties, within the limits set out in this law.

(4) Supervisory authorities and self-regulatory bodies shall implement a risk-based approach. In implementing this approach, the supervisory authorities and self-regulatory bodies shall:

(a) ensure that they have a clear understanding of the risks of money laundering and terrorist financing that exist in Luxembourg;

(b) have on-site and off-site access to all relevant information on the specific domestic and international risks associated with the customers, products and services of professionals; and

(c) base the frequency and intensity of on-site and off-site supervision of professionals on:

(i) the money laundering and terrorist financing risks and the internal policies, controls and procedures of the professional or of the group to which it belongs identified as part of the assessment of the risk profile of the professional or group carried out by the supervisory authority or self-regulatory body;

(ii) the characteristics of the professionals subject to this law and of their financial groups, in particular the range and number of professionals and the degree of discretion they are afforded under the risk-based approach; and

(iii) the risks of money laundering and terrorist financing that exist in Luxembourg.

When assessing the risks of money laundering and terrorist financing, supervisory authorities and self-regulatory bodies shall take into account the factors of potentially higher-risk situations set out in Annex IV.

(5) The assessment of the money laundering and terrorist financing risk profile of professionals, including the risks of non-compliance, shall be reviewed by the supervisory authorities and by self-regulatory bodies both periodically and when major events or changes in their management and activities occur.

(6) The supervisory authorities and self-regulatory bodies shall take into account the margin of discretion allowed to the professional, and appropriately review the risk assessments underlying this discretion, as well as the adequacy and implementation of internal policies, controls and procedures.

Art. 8-2. Supervisory powers of the supervisory authorities

(1) For purposes of the application of this law, the supervisory authorities shall be given all supervisory and investigatory powers necessary for the exercise of their functions within the limits defined in this law.

The powers of supervisory authorities referred to in the first subparagraph include the right to:

(a) have access to any document in any form whatsoever, and to receive or take a copy of it;

(b) request information from any person and, where necessary, to summon any person subject to their respective supervisory powers in accordance with Article 2-1 and to question him in order to obtain information;

(c) carry out on-site inspections or investigations, and also to seize any document, electronic file or other element which would appear useful for ascertaining the truth, from persons subject to their respective supervisory powers in accordance with Article 2-1;

(d) require telephonic recordings, electronic communications or data traffic records held by persons subject to their respective supervisory powers in accordance with Article 2-1;

(e) require persons subject to their respective supervisory powers in accordance with Article 2-1 to cease any practice that is contrary to Articles 2-2 to 5 and 8-3(3), or to their implementing measures, and to abstain from repeating such practice within the period determined by them;

(f) request the freezing or the sequestration of assets from the President of the district court (*tribunal d'arrondissement*) of and in Luxembourg ruling on request;

(g) impose a temporary ban, for a period not to exceed 5 years, on professional activity as regards persons subject to the prudential supervision of the relevant supervisory authority, and as regards members of the management body, employees and tied agents relating to these persons;

(h) require *réviseurs d'entreprises* and *réviseurs d'entreprises agréés* of persons subject to their respective supervisory powers in accordance with Article 2-1 to provide information;

(i) refer information to the State Prosecutor for criminal prosecution;

(j) require *réviseurs d'entreprises*, *réviseurs d'entreprises agréés* or experts to carry out on-site verifications or investigations of persons subject to their respective supervisory powers in accordance with Article 2-1. These verifications and investigations shall be carried out at the expense of the person concerned.

(2) When imposing the injunction provided for in paragraph (1), point (e), the supervisory authorities may impose a penalty payment upon the professionals subject to this measure to compel these persons to act upon the injunction. The amount of the penalty payment, on the grounds of an observed failure to perform, may not be greater than EUR 1,250 per day, with the understanding that the total amount imposed due to an observed failure to perform may not exceed EUR 25,000.

(3) If by the end of the period prescribed by the supervisory authorities pursuant to paragraph (1), point (e), the situation in question has not been remedied, a supervisory authority may as regards the persons subject to its prudential supervision:

(a) suspend the members of the management body or any other person who, by their actions, negligence or lack of prudence, have brought about the situation found to exist and the continued exercise of whose functions may prejudice the implementation of recovery or reorganisation measures;

(b) suspend the exercise of voting rights attaching to shares or units held by shareholders or members whose influence is likely to operate to the detriment of the prudent and sound management of the person or which are held responsible for the practice in breach of Articles 2-2 to 5 and 8-3(3) and for their implementing measures;

(c) suspend the pursuit of that person's business or, if the situation found to exist concerns a particular sector of business, the pursuit of the latter.

(4) The powers of the AED referred to in paragraph (1), first subparagraph, include the right to rely on all databases which it is responsible for processing and to obtain all the information required to assess whether a professional is complying with its professional obligations under this law.

For the purposes of the first subparagraph, the AED shall have access to the trade and companies register.

The minister of the economy shall communicate to the AED a list of professionals which have a business authorisation and which are subject to the supervisory powers of the AED in accordance with Article 2-1(8).

(5) In order to ensure the supervision of professionals provided for in Article 2, point (14a), the AED and the customs administration shall cooperate closely and shall be authorised to exchange the information required to fulfil their respective duties.

Art. 8-2a. Supervisory powers of self-regulatory bodies

(1) For the purposes of the application of this law, the competent bodies within the self-regulatory bodies shall have the following supervisory and investigatory powers:

(a) have access to any document in any form whatsoever, and to receive or take a copy of it;

(b) request information from any person and, where necessary, to summon any person subject to their respective supervisory powers in accordance with Article 2-1 and to hear that person in order to obtain information;

(c) carry out on-site inspections or investigations, and also to seize any document, electronic file or other element which would appear useful for ascertaining the truth, from persons subject to their respective supervisory powers in accordance with Article 2-1;

(d) order the submission of telephone recordings and electronic communications held by persons subject to their respective supervisory powers in accordance with Article 2-1;

(e) require persons subject to their respective supervisory powers in accordance with Article 2-1 to cease any practice that is contrary to Articles 2-2 to 5 and 8-3(3), or to their implementing measures, and to abstain from repeating such practice within the period determined by them;

(f) request the freezing or the sequestration of assets from the President of the district court (*tribunal d'arrondissement*) of and in Luxembourg ruling on request;

(g) prohibit, in the event of a serious breach of professional obligations and if the particular circumstances so require, on a preliminary basis and until a disciplinary body makes an official decision on the matter, the professional activities of persons subject to the supervision of the relevant self-regulatory body, and of members of management bodies, effective directors (*dirigeants*) or other persons subject to their supervisory powers; such prohibition shall cease by operation of law (*ipso jure*) if no referral has been made to the disciplinary body within the months from the date the measure was taken;

(h) require *réviseurs d'entreprises* and *réviseurs d'entreprises agréés* of persons subject to their respective supervisory powers in accordance with Article 2-1 to provide information;

(i) refer information to the State Prosecutor for criminal prosecution;

(j) require *réviseurs d'entreprises*, *réviseurs d'entreprises agréés* or experts to carry out on-site verifications or investigations of persons subject to their respective supervisory powers in accordance with Article 2-1.

These verifications and investigations shall be carried out at the expense of the person concerned.

(2) When imposing the injunction provided for in paragraph (1), point (e), the competent bodies within the self-regulatory bodies may impose a penalty payment upon the professionals subject to this measure to compel these persons to act upon the injunction. The amount of the penalty payment, on the grounds of an observed failure to perform, may not be greater than EUR 1,250 per day, with the understanding that the total amount imposed due to an observed failure to perform may not exceed EUR 25,000.

(3) A full judicial appeal may be filed before the administrative court (*tribunal administratif*) against the decisions of self-regulatory bodies made in accordance with this article. The appeal shall be filed within one month from the notification of the disputed decision, or otherwise shall be time-barred. By way of derogation from the legislation on rules of procedure before the administrative courts, no more than one statement may be submitted by each party, including the initiating application. The response shall be submitted within 14 days of the service of the initiating application. The court shall rule within one month of the request.

Art. 8-3. Reporting of breaches to the supervisory authorities and self-regulatory bodies

(1) The supervisory authorities and self-regulatory bodies shall establish effective and reliable mechanisms to encourage reporting of potential or actual breaches of professional obligations as regards the fight against money laundering and terrorist financing by professionals subject to their respective supervisory powers in accordance with Article 2-1.

To this purpose, they shall provide the persons with one or more secure communication channels, to be used for reporting referred to in the first subparagraph. These channels shall ensure that the identity of persons providing information is known only to the supervisory authority or self-regulatory body to which the information is being provided.

(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, who report breaches committed within a legal person subject to the supervisory powers of the supervisory authorities or self-regulatory bodies in accordance with Article 2-1;

(c) appropriate protection for the accused person;

(d) protection of the personal data concerning both the person who reports the breach and the natural person who is allegedly responsible for a breach, in accordance with Regulation (EU) 2016/679;

(e) clear rules that ensure that confidentiality is guaranteed in all cases in relation to the person who reports breaches referred to in paragraph (1), unless disclosure is required by law.

(3) Persons, including a professional's employees and representatives, shall not be subject to threats, retaliatory measures or hostile acts, and particularly adverse or discriminatory measures with respect to employment, for having reported suspicions of money laundering or terrorist financing internally, to a supervisory authority or to a self-regulatory body.

Persons who are exposed to threats, retaliatory measures, hostile acts, or adverse or discriminatory measures with respect to employment for having reported suspicions of money laundering or terrorist financing to the FIU shall have the right to file a complaint with the supervisory authority or self-regulatory body referred to in Article 2-1.

Any contractual provision or act that runs contrary to the first subparagraph in this section, and in particular any termination of an employment contract in violation of that subparagraph, is null and void by operation of law (*ipso jure*).

If an employee's employment contract is thus terminated, the employee may make recourse as provided for in Article L. 271-1(4) to (7) of the Labour Code.

Section 2 - Administrative enforcement

Art. 8-4. Administrative sanctions and other administrative measures

(1) Supervisory authorities have the power to impose administrative sanctions and to take other administrative measures provided for in paragraph (2) with regard to professionals subject to their respective supervisory powers in accordance with Article 2-1 which do not comply with the obligations set out in Articles 2-2, 3, 3-1, 3-2, 3-3, 4, 4-1, 5, 7-1 paragraphs (2) and (6), and 7-2 paragraph (1) and 8-3 paragraph (3) or their implementing measures, and with regard to members of their management bodies, their effective directors (*dirigeants*) or other persons responsible for the professional's non-compliance with its obligations.

(2) In case of a breach of the provisions referred to in paragraph (1), the supervisory authorities have the power to impose the following administrative sanctions and to take the following administrative measures:

(a) a warning;

(b) a reprimand;

(c) a public statement specifying the identity of the natural or legal person and the nature of the breach;

(d) where the professional is subject to registration or licensing requirements, the initiation of the procedure for the withdrawal or suspension of the registration or license;

(e) in the case of the CSSF and the CAA, a temporary ban, not to exceed 5 years, on:

(i) exercising a professional activity in the financial sector or carrying out one or several transactions as regards persons subject to their respective supervisory powers in accordance with Article 2-1; or

(ii) exercising management functions within professionals subject to their respective supervisory powers in accordance with Article 2-1 as regards any person exercising managerial responsibilities within such professional or any other natural person held responsible for the breach;

(f) administrative fines with a maximum amount up to twice the amount of the benefit derived from the infringement, where it is possible to determine such amount, or a maximum amount of EUR 1,000,000.

In the cases referred to in the first subparagraph, the AED shall cooperate closely with the minister of the economy. On the basis of a reasoned opinion issued by the director of the AED, the minister of the economy shall decide on the full or temporary withdrawal of the business authorisation, until such time as the director of the AED issues a new opinion, as soon as non-compliance with the provisions referred to in paragraph (1) impacts the professional repute of the director (*dirigeant*).

Where the professional concerned is a gambling service provider, the AED shall cooperate closely with the Minister of Justice. On the basis of a reasoned opinion issued by the director of the AED, the Minister of Justice shall decide on the full or temporary withdrawal of the operating licence, until such time as the director of the AED issues a new opinion, as soon as non-compliance with the provisions referred to in paragraph (1) impacts the professional standing of the director (*dirigeant*).

(3) Where the professional concerned is a credit institution or a financial institution, the maximum amount of the administrative fines referred to in paragraph (2), point (f), shall amount to:

(a) in the case of a legal person, EUR 5,000,000 or 10% of the total annual turnover according to the last available accounts which have been approved by the management body; where the professional is a parent company or a subsidiary of a parent undertaking which is required to prepare consolidated financial accounts in accordance with Article 22 of Directive 2013/34/EU, the relevant total turnover shall be the total annual turnover or the corresponding type of income in accordance with the relevant accounting directives according to the last available consolidated accounts approved by the management body of the ultimate parent company;

(b) in the case of a natural person, EUR 5,000,000.

(4) The supervisory authorities may impose a fine ranging from EUR 250 to EUR 250,000 on natural and legal persons which obstruct the application of their powers provided

for in Article 8-2(1), which fail to act in response to their injunctions imposed in accordance with Article 8-2(1), point (e), or which have intentionally provided them with documents or other information which prove to be incomplete, incorrect or false in response to requests based on Article 8-2(1).

Supervisory authorities may impose a fine ranging from EUR 250 to EUR 250,000 on professionals subject to their supervisory powers in accordance with Article 2-1 that have not complied with the provisions in Articles 5(4), third subparagraph and 8-3(3), first subparagraph, as well as on members of their management bodies, their effective directors (*dirigeants*) or other persons responsible for the non-compliance with these provisions.

(5) The expenses incurred for the forced recovery of fines shall be borne by the persons on whom such fines were imposed.

Art. 8-5. Exercise of power of sanction

(1) When determining the type and level of administrative sanctions, the supervisory authorities shall take into account all relevant circumstances, including, where applicable;

(a) the gravity and the duration of the breach;

(b) the degree of responsibility of the natural or legal person held responsible for the breach;

(c) the financial situation of the natural or legal person held responsible for the breach, as indicated, for example, by the total turnover of the legal person held responsible or the annual income of the natural person held responsible;

(d) the benefit derived from the breach by the natural or legal person held responsible, insofar as they can be determined;

(e) the losses for third parties caused by the breach, insofar as they can be determined;

(f) the degree of cooperation on the part of the natural or legal person held responsible for the breach with the supervisory authorities, self-regulatory bodies and the Financial Intelligence Unit;

(g) previous breaches committed by the natural or legal person held responsible;

(h) any potential systemic consequences of the breach.

(2) Where they exercise their power to impose administrative sanctions and measures, the supervisory authorities shall cooperate closely amongst themselves, with self-regulatory bodies and with their foreign counterparts to ensure that the administrative sanctions or measures produce the intended results, and shall coordinate their actions in the case of cross-border matters.

Art. 8-6. Publication of decisions by the supervisory authorities

(1) Supervisory authorities shall publish on their official website all decisions that have been decided or that have acquired the force of *res judicata* (*force de chose décidée* or *force de chose jugée*) imposing a sanction or an administrative measure as a consequence of a breach of the provisions set out in Article 8-4(1) immediately after the person sanctioned has been informed of such decision. This publication shall indicate the type and nature of the breach committed and the identity of the person responsible for it.

The supervisory authorities shall assess on a case-by-case basis the proportionality of the publication of the identity of the persons responsible referred to in the first subparagraph or of the personal data of these persons. Where it considers such publication to be disproportionate or where such publication jeopardises the stability of the financial markets or an ongoing investigation, the supervisory authorities shall:

(a) delay the publication of the decision to impose a sanction or an administrative measure until such time as reasons for not publishing it cease to exist;

(b) publish the decision to impose a sanction or an administrative measure on an anonymous basis if such anonymous publication ensures an effective protection of the personal data concerned; in the case of a decision to publish a sanction or an administrative measure on an anonymous basis, the publication of the relevant data may be postponed for a reasonable period of time if it is foreseen that within that period the reasons for anonymous publication shall cease to exist;

(c) not publish the decision to impose a sanction or an administrative measure, where the options set out in points (a) and (b) are considered insufficient to ensure:

(i) that the stability of the financial markets would not be put in jeopardy; or

(ii) the proportionality of the publication of the decision with regard to measures deemed to be of a minor nature.

(2) Supervisory authorities shall ensure that any document published in accordance with this article shall remain on their official website for a period of five years after its publication. However, personal data contained in the published document shall only be kept on the official website of the supervisory authority for a maximum period of 12 months.

Art. 8-7. Administrative recourse

A full judicial appeal may be filed before the administrative court (*tribunal administratif*) against the decisions of supervisory authorities made in accordance with this chapter. The appeal shall be filed within one month from the notification of the disputed decision, or otherwise shall be time-barred.

Art. 8-8. Provision of information to the European Supervisory Authorities

The supervisory authorities shall inform the European Supervisory Authorities of any administrative sanctions and measures imposed on credit institutions and on financial institutions in accordance with Article 8-4, including any appeal in relation thereto and the outcome thereof.

The supervisory authorities shall check the existence of a relevant conviction in the criminal record of the person concerned. Any exchange of information for those purposes shall be carried out in accordance with the law of 29 March on the organisation of the criminal record, as amended.

Art. 8-9. Recovery of financial sanctions by the AED

(1) The AED has the following means at its disposal to recover debts resulting from sanctions and other administrative measures which it has adopted in accordance with this law:

(a) a right of enforcement by administrative constraint;

(b) the right to register of a mortgage pursuant to the administrative constraint;

(c) the right to issue a summons to a third party holder in accordance with Article 8 of the law of 27 November 1933 on the recovery of direct contributions, excise duties on spirits and social security contributions, as amended.

(2) The first act in the proceedings for the recovery of debts by the AED pursuant to this law is a constraint issued by the receiver of the revenue office responsible for its recovery or his delegate. The constraint is signed and made enforceable by the director of the AED or by his delegate.

It is served by a writ of bailiff or by an agent of the AED or by post. Legal interest shall be due from the day on which the constraint is served.

(3) The enforcement of the constraint may only be interrupted by a reasoned opposition with a summons to appear on a determined date (*assignation à jour fixe*) before the district court (*tribunal d'arrondissement*) of Luxembourg sitting in civil matters.

The writ containing the opposition shall be served on the State in the person of the civil servant who has issued the constraint. The opposition to the constraint may only be based on formal nullities in the constraint or the command or on reasons relating to the extinguishment of the debt.

(4) In case of distraint (*saisie-exécution*), such action shall be undertaken by a bailiff or by an agent of the AED in accordance with the New Code of Civil Procedure.

(5) Acts relating to proceedings, including the constraints and commands, the acts of seizure and the procedural acts to which the recovery of the debts of the AED give rise shall be exempt from stamp and registration duties.

Section 3 – Enforcement by self-regulatory bodies

Art. 8-10. Sanctions and other enforcement measures

(1) The competent bodies within self-regulatory bodies have the power to impose sanctions and to take other measures provided for in paragraph (2) with regard to professionals subject to their respective supervisory powers in accordance with Article 2-1 which do not comply with the obligations set out in Articles 2-2, 3, 3-1, 3-2, 3-3, 4, 4-1, 5 and 8-3 paragraph (3) or their implementing measures, and with regard to members of their management bodies, their effective directors (*dirigeants*) or other persons subject to their supervisory powers who are responsible for the professional's non-compliance with its obligations.

(2) In case of a breach of the provisions referred to in paragraph (1), the competent bodies within the self-regulatory bodies have the power to impose the following sanctions and to take the following measures:

(a) a warning;

(b) a reprimand;

(c) a public statement specifying the identity of the natural or legal person and the nature of the breach;

(d) a temporary ban, for a period not to exceed five years, on the following:

(i) carrying on one or several of the activities listed in Article 1(8) and point 12 of Article 2(1);

(ii) exercising management functions within professionals subject to their respective supervisory powers in accordance with Article 2-1 as regards any person exercising managerial responsibilities within such professional or any other natural person held responsible for the breach;

(e) the temporary suspension, for a period not to exceed five years, of the right to practice the profession;

(f) a lifetime bar from practising the profession, or removal from office;

(g) fines with a maximum amount up to twice the amount of the benefit derived from the infringement, where that benefit can be determined, or a maximum amount of EUR 1,000,000.

(3) The competent bodies within self-regulatory bodies may impose a fine ranging from EUR 250 to EUR 250,000 on persons subject to their supervisory powers which obstruct the application of their powers pursuant to Articles 8-2a paragraph (1), which do not follow injunctions imposed pursuant to Article 8-2a paragraph (1), point (e), or which have intentionally provided them with documents or other information that prove to be incomplete, incorrect or false in response to requests pursuant to Article 8-2a paragraph (1).

Self-regulatory bodies may impose a fine ranging from EUR 250 to EUR 250,000 on professionals subject to their supervisory powers in accordance with Article 2-1 which do not comply with the prohibition set out in Article 8-3(3), first subparagraph, as well as on members of their management bodies, their effective directors (*dirigeants*) or other persons responsible for the non-compliance with this prohibition.

Art. 8-11. Exercise of power of sanction

(1) When determining the type and severity of sanctions, self-regulatory bodies shall take into account all the relevant circumstances, including, where applicable;

(a) the gravity and the duration of the breach;

(b) the degree to which the person held responsible for the breach was responsible for it;

(c) the financial situation of the person held responsible for the breach, as indicated, for example, by the total turnover of the legal person held responsible or the annual income of the natural person held responsible;

(d) the benefit derived from the breach by the person held responsible, insofar as they can be determined;

(e) the losses to third parties caused by the breach, insofar as they can be determined;

(f) the degree of cooperation on the part of the person held responsible for the breach with the self-regulatory bodies, the supervisory authorities and the FIU;

(g) previous breaches committed by the person held responsible;

(h) any potential systemic consequences of the breach.

(2) Where they exercise their power to impose sanctions and other measures, self-regulatory bodies shall cooperate closely amongst themselves, with the supervisory authorities and with their foreign counterparts to ensure that the sanctions or administrative measures produce the intended results, and shall coordinate their actions in the case of cross-border matters.

Art. 8-12. Publication of decisions by self-regulatory bodies

(1) Self-regulatory bodies shall publish on their official website all decisions that have been decided or that have acquired the force of *res judicata* (*force de chose décidée* or *force de chose jugée*) imposing a sanction or an enforcement measure as a consequence of a breach of the provisions set out in Article 8-10(1) immediately after the person sanctioned has been informed of such decision. This publication shall indicate the type and nature of the breach committed and the identity of the person responsible for it.

(2) Self-regulatory bodies shall assess on a case-by-case basis the proportionality of the publication of the identity of the persons responsible referred to in (1) or of the personal data of these persons. Where it considers such publication to be

disproportionate or where such publication jeopardises the stability of the financial markets or an ongoing investigation, the self-regulatory bodies shall:

(a) delay the publication of the decision to impose a sanction or an administrative measure until such time as reasons for not publishing it cease to exist;

(b) publish the decision to impose a sanction or an enforcement measure on an anonymous basis, if such anonymous publication ensures an effective protection of the personal data concerned; in the case of a decision to publish a sanction or an enforcement measure on an anonymous basis, the publication of the relevant data may be postponed for a reasonable period of time if it is foreseen that within that period the reasons for anonymous publication shall cease to exist;

(c) not publish the decision to impose a sanction or an enforcement measure, where the options set out in points (a) and (b) are considered insufficient to ensure:

(i) that the stability of the financial markets would not be put in jeopardy; or

(ii) the proportionality of the publication of the decision with regard to measures deemed to be of a minor nature.

(3) The self-regulatory bodies shall ensure that any document published in accordance with this article shall remain on their official website for a period of five years after its publication. However, personal data contained in the published document shall only be kept on the official website of the self-regulatory body for a maximum period of twelve months.

Art. 8-13. Recovery of fines, penalty payments and other expenses

(1) In the case of a fine referred to in Article 8-10 or a penalty payment referred to in Article 8-2a, paragraph (2), expenses incurred in the enforced recovery of fines shall be borne by the sanctioned person.

(2) The fines, penalty payments and expenses referred to in paragraph (1) are recovered by the AED.

(3) All sums recovered in fines, penalty payments and expenses referred to in paragraph (1) are paid to the National Treasury.

By way of derogation from the preceding subparagraph, 50% of the sum shall be paid to the relevant self-regulatory body, whereby the total amount paid to the self-regulatory body shall not exceed EUR 50,000.

Art. 8-14. Annual report

Self-regulatory bodies shall publish an annual report containing information on:

(a) the measures taken pursuant to the provisions in this section;

(b) the number of reports received of breaches as referenced in Article 8-3, if any;

(c) the number of reports received by the self-regulatory body with respect to Articles 5 and 7 and the number of reports forwarded by the self-regulatory body to the FIU, if any;

(d) where applicable, the number and description of measures taken pursuant to the provisions in section 1 of this chapter to monitor the compliance of the professionals subject to their respective supervisory powers with their obligations pursuant to the following articles:

(i) Articles 2-2, 3, 3-1 and 3-2 (customer due diligence);

(ii) Article 5 (reporting suspicious transactions);

(iii) Article 3(6) (record keeping);

(iv) Articles 4 and 4-1 (internal monitoring).

Chapter 4: Criminal sanctions

Art. 9.

A fine of between EUR 12,500 and EUR 5,000,000 shall be imposed on any person who knowingly contravenes the provisions of Articles 2-2, 3, 3-1, 3-2, 3-3, 4, 4-1, 5, 7-1 paragraphs (2) and (6), 7-2 paragraph (1) and 8-3, paragraph (3).

Title I-1:

National and international cooperation

Chapter 1: National cooperation

Art. 9-1. Cooperation between the FIU, supervisory authorities and self-regulatory bodies

The FIU, the supervisory authorities and the self-regulatory bodies shall cooperate closely amongst themselves.

For the purposes of the first subparagraph, the FIU, the supervisory authorities and the self-regulatory bodies shall be authorised to exchange the information necessary for the performance of their respective duties as regards the fight against money laundering and terrorist financing. The FIU, the supervisory authorities and the self-regulatory bodies shall use the information exchanged exclusively for the performance of these duties.

The exchange of information is subject to the condition that it be used only for the purpose for which it was sought or provided, except with the express prior consent of the one who provided it to use it for other purposes. By the same token, any use of the information for purposes other than, or exceeding, those originally approved requires the express prior consent of the one who provided the information.

Without prejudice to the relevant cases under criminal law, the one who receives the information may not disseminate it to others without the express prior consent of the one who provided it.

The information exchanged is protected by professional secrecy as provided for in Article 458 of the Penal Code or, as the case may be, by professional secrecy as provided for in special legislation. Self-regulatory bodies shall duly empower the persons who process the exchanged information for the purposes of this law. These persons remain subject to secrecy, even after their powers have ended.

The auditors and experts mandated by supervisory authorities or self-regulatory bodies shall be bound by the same professional secrecy, even after the end of their mandate.

Art. 9-1a. Cooperation between the CSSF and the CAA for the purposes of the fight against money laundering and terrorist financing and for the purposes of the prudential supervision of credit institutions and financial institutions or the supervision of financial markets

(1) Without prejudice to Article 9-1 and other legislation governing national cooperation between financial sector supervisory authorities, the CSSF and the CAA shall cooperate closely and shall exchange information with one another or between their respective departments for the purposes of the fight against money laundering and terrorist financing, as well as for the purposes of other legislation related to the regulation and prudential supervision of credit institutions and financial institutions, or related to the supervision of financial markets.

(2) All persons who, for the purposes of this law, work or worked for the CSSF or the CAA are bound by professional secrecy, as are the auditors and experts commissioned by them.

Without prejudice to criminal proceedings, the confidential information received by the persons referred to in the first subparagraph in the performance of their duties pursuant to this law may not be disclosed except in an abridged or consolidated form, such that the different credit institutions and financial institutions cannot be identified.

(3) When receiving confidential information, the CSSF and the CAA may only use it for the following:

(a) to perform the duties incumbent upon them pursuant to this law or to other legislation relating to the fight against money laundering and terrorist financing, the regulation and prudential supervision of credit institutions and financial institutions, or the supervision of financial markets, in particular in order to impose sanctions;

(b) in the context of an appeal against a decision made by the CSSF or CAA, including in judicial proceedings;

(c) in the context of judicial proceedings initiated in accordance with special provisions of European Union law relating to Directive (EU) 2015/849 or to the regulation and prudential supervision of credit institutions and financial institutions, or to the supervision of financial markets.

Any dissemination of this information by the supervisory authority or recipient department to another authority, department or third party, and any use of the information for purposes other than, or exceeding, those originally approved, must be authorised in advance by the authority or department that communicated it.

Art. 9-1b. National cooperation between the CSSF in its capacity as a supervisory authority, the FIU and supervisory authorities

The CSSF, in its capacity as competent authority for the purposes of Article 42 of the law of 5 April 1993 on the financial sector, as amended, the FIU and the supervisory authorities shall cooperate closely within the framework of their respective competences and shall provide each other with information relevant to their respective tasks under this law, under the law of 5 April 1993 on the financial sector, as amended, and under Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, hereinafter "Regulation No 2013/575", provided that such cooperation and exchange of information do not impinge on any ongoing investigation or proceedings.

Chapter 2: International cooperation

Art. 9-2. Cooperation with the European Supervisory Authorities

The supervisory authorities shall provide the European Supervisory Authorities with all the information at their disposal in relation to the performance of their duties provided for in Article 2-1 which are necessary to enable the European Supervisory Authorities to carry out their duties under Directive (EU) 2015/849.

The supervisory authorities shall inform the European Supervisory Authorities of cases where the law of a third country does not permit the implementation of the policies and procedures required pursuant to Article 4-1(1). In such cases, coordinated action may be taken to find a solution. When determining which third countries do not permit the implementation of the policies and procedures required pursuant to Article 4-1(1), the CSSF and the CAA shall take into account any legal constraints likely to obstruct the smooth implementation of those policies and procedures, including with respect to secrecy, data protection and other restrictions limiting the exchange of information that could be useful for the relevant purpose.

Where, in the context of prudential supervision of a CRR institution within the meaning of Article 1(11a) of the law of 5 April 1993 on the financial sector, as amended, a monitoring measure – in particular an assessment of the institution's governance mechanisms, business model or activities – gives the CSSF reasonable grounds to suspect that, in connection with this institution, a money laundering or terrorist financing operation or attempt is ongoing or has occurred, or that there is an increased risk of such an operation or attempt, the CSSF shall immediately inform the European Banking Authority. In the case of an increased risk of money laundering or terrorist financing, the CSSF shall communicate its assessment to the European Banking Authority without delay. This subparagraph is without prejudice to other measures taken by the CSSF in the performance of the duties of prudential supervision incumbent upon it. For the purposes of this subparagraph, the CSSF shall ensure that the departments responsible for prudential supervision and those responsible for the fight against money laundering and terrorist financing cooperate and share information in accordance with Article 9-1a. At the same time, the CSSF shall coordinate in accordance with Article 9-2b with the European Central Bank, acting in compliance with Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions. They shall communicate their joint assessment to the European Banking Authority without delay.

Art. 9-2a. Cooperation of supervisory authorities with their foreign counterparts

(1) Supervisory authorities shall cooperate with their counterparts in other countries where necessary in order to perform their respective duties, and for the purposes of the fight against money laundering and terrorist financing, Directive (EU) 2015/849, this law or the relevant implementing measures. This also applies to the competent counterpart authorities of other Member States or third countries with analogous duties and roles pursuant to a request for cooperation, even where these competent foreign authorities are of a different nature or status. In particular, supervisory authorities shall assist foreign counterpart authorities by sharing information and cooperating in the context of investigations.

(2) Upon request, supervisory authorities shall communicate, in a timely manner, any and all information required for the purposes referred to in paragraph (1).

Before fulfilling a request for information, the supervisory authority to which the request was addressed shall verify that the request for information contains the full facts regarding the instance and, where applicable, legal information and information regarding the degree of urgency, as well as the intended use of the information requested. Where necessary, the supervisory authority to which the request was addressed may ask the requesting counterpart authority for more information regarding the use and utility of the information requested.

Where the supervisory authority receives a request for information which is in accordance with the foregoing, it shall take the necessary measures to collect the requested information without delay, making use of the powers at its disposal by virtue of its statutory powers. If the supervisory authority is unable to provide the requested information in a timely manner, it shall inform the requesting counterpart authority of the reasons for this.

(3) Where a supervisory authority believes that acts which are in breach of the provisions of this law are being, or have been, committed in a Member State or third country, or that acts committed in Luxembourg breach the provisions of Directive (EU) 2015/849 or of applicable domestic legislation in the Member State or third country which contains similar anti-money laundering and counter-terrorist financing provisions and prohibitions, it shall inform the counterpart authority in the relevant Member State or third country of this in as much detail as possible.

(4) The communication of information by supervisory authorities to a foreign counterpart authority is subject to the following conditions:

(a) the information communicated shall be necessary and serve to enable the recipient authority to perform its duties under Directive (EU) 2015/849 or pursuant to that authority's national legislation on the fight against money laundering and terrorist financing;

(b) the information communicated shall be subject to professional secrecy on the part of the recipient authority, and the guarantees offered by that authority's professional secrecy shall be at least equivalent to those offered by the professional secrecy to which the supervisory authorities are subject, in particular with respect to persons working for them in accordance with Article 9-1a paragraph (2);

(c) the authority which receives information from the supervisory authorities shall only use it for the purposes for which it was communicated, and shall be in a position to ensure that no other use of it is made;

(d) where this information originates from other supervisory authorities, other authorities or national authorities bound to secrecy, or other foreign counterpart authorities, it shall only be disclosed with the express consent of those authorities and, where applicable, exclusively for the purposes for which those authorities have given their consent.

(5) When addressing requests for cooperation to foreign counterpart authorities, supervisory authorities shall do everything in their power to provide full factual information and, where applicable, legal information and information regarding the degree of urgency and the intended use of the information requested. Upon request, requesting supervisory authorities shall provide more information regarding the use and utility of the information requested to the counterpart authority to which the request was addressed.

(6) Without prejudice to their obligations in the context of criminal legal proceedings, supervisory authorities which receive confidential information from a foreign counterpart authority shall only use this information for the purposes for which it was requested or provided. In particular, such information may only be used:

(a) to perform the duties incumbent upon them pursuant to this law, Directive (EU) 2015/849 or other anti-money laundering and counter terrorist financing legislation;

(b) in the context of an appeal against a decision made by a supervisory authority, including in judicial proceedings; or

(c) in the context of judicial proceedings initiated in accordance with special provisions of European Union law with respect to this law.

Any dissemination of the information for administrative, judicial, investigatory or prosecutorial purposes exceeding those originally recorded must be authorised in advance by the authority to which the request was addressed.

(7) Supervisory authorities shall ensure an appropriate degree of confidentiality for all requests for cooperation or information transmitted so as to protect the integrity of investigations or queries for information, in compliance with the obligations of both parties concerning the respect for private life and the protection of personal data. Supervisory authorities shall protect the information exchanged in the same manner as they would comparable information received from domestic sources. Information shall be exchanged securely, through trustworthy channels and mechanisms.

Art. 9-2b. Cooperation of supervisory authorities and self-regulatory bodies with their foreign counterparts

Supervisory authorities and self-regulatory bodies shall not reject a request for assistance by a foreign counterpart authority for any of the following reasons:

(a) the request is also deemed to pertain to tax matters;

(b) the law requires professionals to respect professional secrecy or confidentiality, except in cases in which the relevant information sought in the request is protected by confidentiality rules or where professional secrecy applies, as described in Article 7(1);

(c) there is an ongoing investigation or proceeding in Luxembourg, except where the assistance could interfere with that investigation or proceeding;

(d) the requesting counterpart authority is of a different nature or status than the supervisory authority to which the request was addressed.

Art. 9-2c. Cooperation of the CSSF and the CAA with their foreign counterpart authorities for the purposes of the fight against money laundering and terrorist financing and for the purposes of the prudential supervision of credit institutions and financial institutions or the supervision of financial markets

(1) Without prejudice to Article 9-2a and other provisions governing international cooperation between financial sector supervisory authorities, the CSSF and the CAA shall cooperate closely with their counterparts in other countries where necessary in order to perform their respective duties, and for the purposes of the fight against money laundering and terrorist financing, Directive (EU) 2015/849, this law or the relevant implementing measures, as well as for the purposes of other legislation related to the regulation and prudential supervision of credit institutions and financial institutions, or related to the supervision of financial markets. This also applies to the competent counterpart authorities of other Member States or third countries with analogous duties and roles pursuant to a request to cooperate, even where these competent foreign authorities are of a different nature or status.

The CSSF and the CAA shall assist foreign counterpart authorities by sharing information and cooperating in the context of investigations. They shall also exchange information and cooperate with the European Central Bank, acting in compliance with Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions.

(2) The CSSF and the CAA shall communicate, in a timely manner, any and all information required for the purposes referred to in paragraph (1).

Before fulfilling a request for information, the authority to which the request was addressed shall verify that the request for information contains the full facts regarding the instance and, where applicable, legal information and information regarding the degree of urgency, as well as the intended use of the information requested.

Where necessary, the authority to which the request was addressed may ask the requesting counterpart authority for more information regarding the use and utility of the information requested.

Where the supervisory authority receives a request for information which is in accordance with the foregoing, it shall take the necessary measures to collect the requested information without delay, making use of its statutory powers. If the authority to which the request was addressed is unable to provide the requested

information in a timely manner, it shall inform the requesting counterpart authority of the reasons for this.

(3) The communication of information by the CSSF or the CAA to a foreign counterpart authority is subject to the following conditions:

(a) the information communicated shall be necessary and serve to enable the recipient authority to perform its duties under Directive (EU) 2015/849, or pursuant to that authority's national legislation on the fight against money laundering and terrorist financing or on the regulation and prudential supervision of credit institutions and financial institutions or the supervision of financial markets;

(b) the information communicated shall be subject to professional secrecy on the part of the recipient authority, and the guarantees offered by that authority's professional secrecy shall be at least equivalent to those offered by the professional secrecy to which the CSSF and the CAA are subject, in particular with respect to persons working for them in accordance with Article 9-1a paragraph (2);

(c) the authority which receives information from the supervisory authorities shall not use them except for the purposes for which the information was communicated, and shall be in a position to ensure that no other use is made of it;

(d) where this information originates from other supervisory authorities, other authorities or national authorities bound to secrecy, or other foreign counterpart authorities, it shall only be disclosed with the express consent of those authorities and, as applicable, exclusively for the purposes for which those authorities have given their consent.

(4) The provisions in Article 9-2a paragraph (5) shall apply.

(5) When addressing requests for cooperation to their foreign counterparts, the CSSF and the CAA shall do everything in their power to provide full factual information and, where applicable, legal information and information regarding the degree of urgency and the intended use of the information requested. Upon request, they shall provide more information regarding the use and utility of the information requested to the counterpart authority to which the request was addressed.

(6) Without prejudice to the applicable provisions on professional secrecy referred to in Article 9-1a paragraph (2), when receiving confidential information, the CSSF and the CAA may only use it for the following:

(a) to perform the duties incumbent upon them pursuant to this law, or pursuant to other anti-money laundering and counter-terrorist financing legislation, the regulation and prudential supervision of credit institutions and financial institutions, and the supervision of financial markets, in particular in order to impose sanctions;

(b) in the context of an appeal against a decision made by the CSSF or the CAA, including in judicial proceedings; or

(c) in the context of judicial proceedings initiated in accordance with special provisions of European Union law relating to Directive (EU) 2015/849 or to the regulation and prudential supervision of credit institutions and financial institutions, and the supervision of financial markets.

Any dissemination of this information by the recipient supervisory authority to other supervisory authorities or third parties, and any use of the information for purposes other than, or exceeding, those originally approved, must be authorised in advance by the authority that communicated it.

(7) The CSSF and the CAA have the authority to enter into cooperation agreements with their counterparts in third countries which provide for cooperation and the exchange of confidential information. Such cooperation agreements are concluded subject to reciprocity, and only where the information communicated is subject to professional secrecy requirements offering guarantees at least equivalent to the professional secrecy referred to in Article 9-1a paragraph (2). The confidential information exchanged under such agreements shall serve to enable the said authorities to perform their supervisory duties..

Where it originates from an authority in another Member State, the information exchanged shall only be disclosed with the express consent of the authority that shared it and, as applicable, exclusively for the purposes for which that authority has given its consent.

(8) The CSSF and the CAA shall ensure an appropriate degree of confidentiality for all requests for cooperation or information transmitted so as to protect the integrity of investigations or queries for information, in compliance with the obligations of both parties concerning the respect for private life and the protection of personal data. The CSSF and the CAA shall protect the information exchanged in the same manner as they would comparable information received from domestic sources. The exchange of information shall be secure and shall be made through trustworthy channels and mechanisms.

(9) Where it is relevant to the purposes of the fight against money laundering and terrorist financing, the CSSF and the CAA may exchange, in particular, the following types of information with their foreign counterparts, and especially with those counterpart authorities with which they share a common responsibility towards credit institutions or financial institutions that operate within the same group:

(a) regulatory information, e.g. information on national regulations and general information on financial sectors;

(b) prudential information, in particular for supervisory authorities applying the *Core Principles for Effective Banking Supervision* published by the Basel Committee on Banking Supervision, the *Objectives and Principles of Securities Regulation* published by the International Organization of Securities Commissions or the Insurance Core Principles published by the International Association of Insurance Supervisors, including information on the activities of credit institutions and financial institutions, their beneficial owners, their management, their competence and their professional repute;

(c) information relating to the fight against money laundering and terrorist financing, such as information on the internal anti-money laundering and counter-terrorist financing policies and procedures of credit institutions and financial institutions, on customer due diligence, on client files, on selected samples of accounts and on transactions.

Art. 9-2d. International cooperation between the CSSF in its capacity as a supervisory authority, the FIU, supervisory authorities and their counterparts

The CSSF, in its capacity as competent authority for the purposes of Article 42 of the law of 5 April 1993 on the financial sector, as amended, the FIU and the supervisory authorities shall cooperate closely with their counterparts in the other Member States within their respective competences and shall communicate to them the information relevant to their respective tasks under Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures, hereinafter "Directive 2013/36/EU", Regulation (EU) No 575/2013 and Directive (EU) 2015/849, provided that such cooperation and exchange of information does not impinge on any ongoing investigation or proceedings.

TITLE I-II:

Appeal against instructions of the Financial Intelligence Unit

Art. 9-3.

(1) Any person who has a right over property covered by an instruction by the Financial Intelligence Unit not to execute transactions under Article 5(3), and the professional concerned by this instruction, may make application for execution of the transactions by submitting a request to the council chamber of the Luxembourg district court (*tribunal d'arrondissement*).

(2) The request shall be communicated to the Financial Intelligence Unit and the State Prosecutor within 24 hours of its delivery to the registry of the council chamber.

(3) The Financial Intelligence Unit shall prepare a written and reasoned report justifying the instruction issued pursuant to Article 5(3) and shall transmit it to the registry of the council chamber within five days of the delivery of the request. This report shall be communicated by the registry of the council chamber to the State Prosecutor and to the applicant.

(4) The council chamber may request or authorise a judge of the Financial Intelligence Unit to make oral submissions.

(5) The council chamber shall make a ruling on the basis of the report submitted pursuant to paragraph (3), the submissions made pursuant to paragraph (4) and after hearing the State Prosecutor and the applicant.

(6) The order of the council chamber is subject to appeal by the State Prosecutor or by the applicant in the manner and within the time limits set out in Article 133 et seq. of the Code of Criminal Procedure.

TITLE II

Amending, repealing and miscellaneous provisions

[***]

Art. 25.

This law may be referred to in abbreviated form using the designation “law on the fight against money laundering and terrorist financing”.

Art. 26. Repealed[5]

Art. 27. Repealed[6]

Art. 28. Repealed[7]

[5] Law of 13 February 2018.
[6] Ibidem.
[7] Ibidem.

ANNEX I

Activities and transactions referred to in Article 1 (3a), point (e):

1. Acceptance of deposits and other repayable funds from the public, including private banking.

2. Lending, including consumer credit, mortgage credit, factoring, with or without recourse, financing of commercial transactions (including forfeiting).

3. Financial leasing, not including financial leasing arrangements in relation to consumer products.

4. Payment services within the meaning of point (3) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

5. Transfer services of funds or securities insofar as this activity is not covered by point 4. This shall apply to financial services that consist of accepting cash, cheques or any other payment instrument or value deposit and paying an equivalent amount in cash or any other form to a beneficiary by means of a communication, message, transfer or clearing system to which the money or securities transfer service belongs. Transactions carried out through these services may involve one or more intermediaries and a third party receiving the final payment, and may include any new means of payment. This does not include the exclusive provision of messages or any other support system for the purpose of transferring funds to financial institutions.

6. Issuance and management of means of payment (such as cheques, traveller's cheques, money orders and bank drafts, letters of credit) insofar as this activity is not covered by points 4 or 15.

7. Financial guarantees and commitments.

8. Trading and transactions for the institution's own account or on behalf of its customers in:

   (a) money market instruments (such as cheques, bills, notes, certificates of deposit and derivatives, among others);

   (b) foreign exchange;

   (c) exchange, interest-rate and index instruments;

   (d) transferable securities;

   (e) commodity futures trading;

   (f) futures and options.

9. Participation in securities issues and the provision of financial services related to such issues.

10. Advice to companies on capital structure, industrial strategy and related matters and advice and services in mergers and acquisitions.

11. Intermediation on interbank markets

12. Individual and collective wealth management or wealth management consulting.

13. Safekeeping and administration of cash or liquid securities on behalf of other persons.

14. Safe-deposit box rental

15. Issue and management of electronic money.

16. Otherwise investing, administering or managing funds or money on behalf of other persons.

17. Underwriting and placement of life insurance and other investment-related insurance, by either insurance undertakings or insurance intermediaries (agents and brokers).

18. Money and currency changing.

ANNEX II

The following is a non-exhaustive list of risk variables that professionals shall consider when determining to what extent to apply customer due diligence measures in accordance with Article 3(2a):

(i) the purpose of an account or relationship;

(ii) the level of assets to be deposited by a customer or the size of transactions undertaken;

(iii) the regularity or duration of the business relationship.

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 3-1(2), subparagraph 2:

(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 in countries or territories with low levels of corruption;

(c) customers that are 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 for which the premium is low;

(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 (among other things: certain types of electronic money);

(3) Geographical risk factors – being registered, established or domiciled in:

(a) Member States;

(b) third countries having effective fight anti-money laundering and terrorist financing systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which, on the basis of credible 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 revised FATF Recommendations and effectively implement those requirements.

ANNEX IV

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 3-2(1), subparagraph 2:

(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) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(g) third-country customers seeking rights of residence or citizenship by means of transfers of funds, the purchase of property or government bonds, or investment in private companies.

(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 electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, 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 artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

(3) Geographical risk factors:

(a) without prejudice to Article 3-2(2), countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.