



EUROPEAN PARLIAMENT

2009 – 2014

Consolidated legislative document

11.3.2014

EP-PE_TC1-COD(2013)0025

*****I**

POSITION OF THE EUROPEAN PARLIAMENT

adopted at first reading on 11 March 2014 with a view to the adoption of Directive 2014/.../EU of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
(EP-PE_TC1-COD(2013)0025)

PE 505.540

EN

United in diversity

EN

POSITION OF THE EUROPEAN PARLIAMENT

adopted at first reading on 11 March 2014

with a view to the adoption of Directive 2014/.../EU of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Central Bank¹,

Having regard to the opinion of the European Economic and Social Committee²,

Acting in accordance with the ordinary legislative procedure³,

¹ OJ C 166, 12.6.2013, p. 2.

² OJ C 271, 19.9.2013, p. 31.

³ Position of the European Parliament of 11 March 2014.

Whereas:

- (1) Massive flows of ~~dirty~~ **illicit** money can damage the stability and reputation of the financial sector and threaten the internal market; and ~~terrorism~~ **international development. Terrorism** shakes the very foundations of our society. **The key facilitators of illicit money flows are secretive corporate structures operating in and through secrecy jurisdiction, often also referred to as tax havens.** In addition to ~~further developing~~ the criminal law approach, ~~a preventive effort~~ **at Union level, prevention** via the financial system **is indispensable and** can produce **complementary** results. **However, the preventive approach should be targeted and proportional, and should not result in the establishment of a comprehensive system for controlling the entire population.** [Am. 1]

- (2) The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. In order to facilitate their criminal activities, money launderers and terrorist financiers could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the integrated financial area entails, ~~if~~. **Therefore**, certain coordinating measures are ~~not adopted~~ **necessary** at Union level. **At the same time, the objectives of protection of society from criminals and protection of the stability and integrity of the European financial system should be balanced against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs. Any requirement imposed on obliged entities to fight money laundering and terrorist financing should therefore be justified and proportionate.** [Am. 2]

- (3) The current proposal is the fourth directive to deal with the threat of money laundering. Council Directive 91/308/EEC¹ defined money laundering in terms of drugs offences and imposed obligations solely on the financial sector. Directive 2001/97/EC of the European Parliament and of the Council² extended the scope both in terms of the crimes covered and the range of professions and activities covered. In June 2003 the Financial Action Task Force (FATF) revised its Recommendations to cover terrorist financing, and provided more detailed requirements in relation to customer identification and verification, the situations where a higher risk of money laundering may justify enhanced measures and also situations where a reduced risk may justify less rigorous controls.

¹ Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (OJ L 166, 28.6.1991, p. 77).

² Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (OJ L 344, 28.12.2001, p. 76).

Those changes were reflected in Directive 2005/60/EC of the European Parliament and of the Council¹ and Commission Directive 2006/70/EC². ***In implementing the FATF Recommendations, the Union should fully respect its data protection law, as well as the Charter of Fundamental Rights of the European Union (Charter) and the European Convention for the Protection of Human Rights and Fundamental Freedoms. [Am. 3]***

¹ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309, 25.11.2005, p. 15).

² Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (OJ L 214, 4.8.2006, p. 29).

- (4) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even Union level, without taking account of international coordination and cooperation, would have very limited effects. The measures adopted by the Union in that field should therefore be ~~consistent with~~ ***compatible with, and at least as stringent as,*** other action undertaken in ~~other~~ ***the*** international fora. ***Avoiding tax and mechanisms of non-disclosure and concealment can be used as strategies employed in money laundering and terrorist financing in order to avoid detection.*** Union action should continue to take particular account of the FATF Recommendations, ~~which constitutes the foremost~~ ***and the recommendations of other*** international ~~body~~ ***bodies*** active in the fight against money laundering and terrorist financing. With a view to reinforce the efficacy of the fight against money laundering and terrorist financing, Directives 2005/60/EC and 2006/70/EC should, ***where appropriate,*** be aligned with the new FATF Recommendations adopted and expanded in February 2012. ***However, it is essential for such an alignment with the non-binding FATF Recommendations to be carried out in full compliance with Union law, especially as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter.*** [Am. 4]

(4a) Particular attention should be paid to the fulfilment of the obligations set out in Article 208 of the Treaty on the Functioning of the European Union (TFEU), which requires coherence in development cooperation policy in order to stem the increasing trend of money laundering activities being moved from developed countries to developing countries with less stringent anti-money laundering law. [Am. 5]

(4b) In view of the fact that illicit financial flows, and in particular money laundering, represent between 6 and 8,7 % of the GDP of developing countries¹, which is an amount 10 times larger than the assistance by the Union and its Member States to the developing world, the measures taken to combat money laundering and terrorist financing need to be coordinated and to take into account the Union's and the Member States' development strategy and policies which aim to fight against capital flight. [Am. 6]

¹ Sources: "Tax havens and development. Status, analyses and measures", NOU, Official Norwegian Reports, 2009.

- (5) Furthermore, the misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures of this Directive should cover ~~not only~~ the manipulation of money derived from *serious* crime ~~but also~~ **and** the collection of money or property for terrorist purposes. [Am. 7]
- (5a) *Irrespective of the penalties provided for in the Member States, the primary objective of all measures taken under this Directive should be to combat all practices which result in substantial illegal profits being generated. It should do so by taking all possible steps to prevent the financial system from being used to launder those profits.* [Am. 8]
- (6) The use of large cash payments is vulnerable to money laundering and terrorist financing. In order to increase vigilance and mitigate the risks posed by cash payments natural and legal persons ~~trading in goods~~ should be covered by this Directive to the extent that they make or receive cash payments of EUR 7 500 or more. Member States should be able to decide to adopt stricter provisions including a lower threshold. [Am. 9]

(6a) *Electronic money products are increasingly used as a substitute for bank accounts. The issuers of such products should be under a strict obligation to prevent money laundering and terrorist financing. However, it should be possible to exempt electronic money products from customer due diligence if certain cumulative conditions are met. The use of electronic money that is issued without performing customer due diligence should be allowed for the purchase of goods and services only from merchants and providers who are identified and whose identification is verified by the electronic money issuer. For person-to-person transfers, the use of electronic money without performing customer due diligence should not be allowed. The amount stored electronically should be sufficiently small in order to avoid loopholes and to make sure that a person cannot obtain an unlimited amount of anonymous electronic money products. [Am. 10]*

(6b) *Estate agents are active in many different ways in the field of property transactions in the Member States. In order to reduce the risk of money laundering in the property sector estate agents should be included within the scope of this Directive where they are involved in financial transactions relating to property as part of their professional activities. [Am. 11]*

- (7) Legal professionals, as defined by the Member States, should be subject to the provisions of this Directive when participating in financial or corporate transactions, including providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing. There should, however, be exemptions from any obligation to report information obtained either before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Thus, legal advice should remain subject to the obligation of professional secrecy unless the legal counsellor is taking part in money laundering or terrorist financing, the legal advice is provided for money laundering or terrorist financing purposes or the lawyer knows that the client is seeking legal advice for money laundering or terrorist financing purposes.

- (8) Directly comparable services should be treated in the same manner when provided by any of the professionals covered by this Directive. In order to ensure respect for the rights guaranteed by the Charter, in the case of auditors, external accountants and tax advisors, who, in some Member States, may defend or represent a client in the context of judicial proceedings or ascertain a client's legal position, the information they obtain in the performance of those tasks should not be subject to the reporting obligations in accordance with this Directive.

- (9) It is important to highlight expressly that ‘tax crimes’ relating to direct and indirect taxes are included in the ~~broad~~ definition of ‘criminal activity’ under this Directive in line with the revised FATF Recommendations. *The European Council of 23 May 2013 stated the need to deal with tax evasion and fraud and to fight money laundering in a comprehensive manner, both within the internal market and vis-à-vis non-cooperative third countries and jurisdictions. Agreeing on a definition of tax crimes is an important step in detecting those crimes, as too is public the disclosure of certain financial information by large companies operating in the Union on a country-by-country basis. It is also important to ensure that obliged entities and legal professionals, as defined by Member States, do not seek to frustrate the intent of this Directive or to facilitate or to engage in aggressive tax planning.* [Am. 12]
- (9a) *Member States should introduce General Anti-Avoidance Rules (GAAR) on tax matters with a view to curbing aggressive tax planning and avoidance in accordance with the European Commission's recommendations on Aggressive Tax Planning on December 12th 2012 and the OECD Progress Report to the G20 on 5 September 2013.* [Am. 13]

- (9b) *When they are performing or facilitating commercial or private transactions, entities which have a specific role in the financial system, such as the European Investment Bank (EIB), the European Bank for Reconstruction and Development (EBRD), the central banks of the Member States and central settlement systems should, as far as possible, observe the rules applicable to other obliged entities adopted pursuant to this Directive. [Am. 14]*
- (10) There is a need to identify any natural person who exercises ownership or control over a legal person. While finding a *specific* percentage shareholding will not automatically result in finding the beneficial owner, it is ~~an evidential~~ *one* factor ~~to be taken into account~~ *among others for the identification of the beneficial owner*. Identification and verification of beneficial owners should, where relevant, extend to legal entities that own other legal entities, and should follow the chain of ownership until the natural person who exercises ownership or control of the legal person that is the customer is found. [Am. 15]

- (11) *It is important to ensure, and to enhance, the traceability of payments.* The need for *existence of* accurate and up-to-date information on the beneficial owner *of any legal entity, such as legal persons, trusts, foundations, holdings and all other similar existing or future legal arrangements* is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. Member States should therefore ensure that companies retain information on their beneficial ownership and make ~~this~~ *adequate, accurate and up-to-date* information available to ~~competent~~ authorities and obliged entities *through central public registers, accessible on-line and in an open and secure data format, in accordance with Union data protection rules and the right to privacy as enshrined in the Charter. Access to such registers should be granted to competent authorities, in particular FIUs and obliged entities, as well as to the public subject to prior identification of the person wishing to access the information and to the possible payment of a fee.* In addition, trustees should declare their status to obliged entities. [Am. 16]

(11a) The establishment of beneficial ownership registers by Member States would significantly improve the fight against money laundering, terrorist financing, corruption, tax crimes, fraud and other financial crimes. This could be achieved by improving the operations of the existing business registers in the Member States. It is vital that registers are interconnected if effective use is to be made of the information contained therein, due to the cross-border nature of business transactions. The interconnection of business registers across the Union is already required by Directive 2012/17/EU of the European Parliament and of the Council¹ and should be further developed. [Am. 17]

¹ ***Directive 2012/17/EU of the European Parliament and of the Council of 13 June 2012 amending Council Directive 89/666/EEC and Directives 2005/56/EC and 2009/101/EC of the European Parliament and of the Council as regards the interconnection of central, commercial and companies register (OJ L 156, 16.6.2012, p. 1).***

- (11b) *Technological progress has provided tools which enable obliged entities to verify the identity of their customers when certain transactions occur. Such technological improvements provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities of Member States and obliged entities should be proactive in combating new and innovative ways of money laundering, while respecting fundamental rights, including the right to privacy and data protection. [Am. 18]***
- (12) This Directive should also apply to those activities of the obliged entities covered by this Directive which are performed on the internet.
- (12a) *The representatives of the Union in the governing bodies of the EBRD should encourage the EBRD to implement the provisions of this Directive and to publish on its website an anti-money laundering policy, containing detailed procedures that would give effect to this Directive. [Am. 19]***

- (13) The use of the gambling sector to launder the proceeds of criminal activity is of concern. In order to mitigate the risks related to the sector and to provide parity amongst the providers of gambling services, an obligation for all providers of gambling services to conduct customer due diligence for single transactions of EUR 2 000 or more should be laid down. ***When carrying out that due diligence a risk based approach should be adopted that reflects the different risks for different types of gambling services and whether they represent a high or low risk for money laundering. The special characteristics of different types of gambling should also be taken into account, by, for example, differentiating between casinos, on-line gambling or other providers of gambling services.*** Member States should consider applying that threshold to the collection of winnings as well as wagering a stake. Providers of gambling services ~~with physical premises (e.g. casinos and gaming houses)~~ should ensure that customer due diligence, if it is taken at the point of entry ~~to the premises,~~ can be linked to the transactions conducted by the customer ~~on those premises.~~ [Am. 20]

(13a) *Money laundering is becoming increasingly sophisticated and also includes illegal, and sometimes legal, betting, in particular in relation to sporting events. New forms of lucrative organised crime like match-fixing have arisen and have developed into a profitable form of criminal activity related to money laundering.*

[Am. 21]

(14) The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a *holistic* risk-based approach *based on minimum standards* should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision making to better target the money laundering and terrorist financing risks facing the Union and those operating within it. [Am. 22]

- (15) Underpinning the risk-based approach is a need for Member States *and the Union* to identify, understand and mitigate the money laundering and terrorist financing risks it faces. The importance of a supra-national approach to risk identification has been recognised at international level, and the European Supervisory Authority (European Banking Authority) ('EBA'), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council¹; the European Supervisory Authority (European Insurance and Occupational Pensions Authority) ('EIOPA'), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council²; and the European Supervisory Authority (European Securities and Markets Authority) ('ESMA'), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council³, should be tasked with issuing an opinion on the risks affecting the financial sector *and, in cooperation with Member States, should develop minimum standards for risk assessments carried out by the competent national authorities. That process should, as far as possible, involve relevant stakeholders through public consultations.* [Am. 23]

¹ Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

² Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

³ Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

- (16) The results of risk assessments ~~at Member State level~~ should, where appropriate, be made available *in a timely manner* to obliged entities to enable them to identify, understand and mitigate their own risks. [Am. 24]
- (17) In order to better understand and mitigate risks at Union level, *a supranational risk analysis should be carried out so that the risks of money laundering and terrorist financing to which the internal market is exposed can be identified effectively. The Commission should require the Member States to deal with scenarios considered to be high risk in an effective way. Furthermore*, Member States should share the results of their risk assessments with each other and with the Commission, EBA, EIOPA ~~and~~, ESMA *(together referred to as the 'ESAs'), and Europol*, where appropriate. [Am. 25]
- (18) When applying the provisions of this Directive, it is appropriate to take account of the characteristics and needs of small obliged entities which fall under its scope, and to ensure a treatment which is appropriate to the specific needs of small obliged entities, and the nature of the business.

- (19) Risk itself is variable in nature, and the variables, either on their own or in combination, may increase or decrease the potential risk posed, thus having an impact on the appropriate level of preventative measures, such as customer due diligence measures. Thus, there are circumstances in which enhanced due diligence should be applied and others in which simplified due diligence may be appropriate.
- (20) It should be recognised that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required.

(21) This is particularly true of business relationships with individuals who hold or have held important public positions, particularly those from countries where corruption is widespread, *within the Union and internationally*. Such relationships may expose the financial sector in particular to significant reputational and legal risks. The international effort to combat corruption also justifies the need to pay special attention to such cases and to apply appropriate enhanced customer due diligence measures in respect of persons who hold or have held prominent functions domestically or abroad and senior figures in international organisations. [Am. 26]

(21a) *The need for enhanced customer due diligence measures in respect of persons who hold or have held prominent functions, whether domestically or abroad, and senior figures in international organisations should not, however, lead to a situation in which lists containing information on such persons are traded for commercial purposes. Member States should take appropriate measures to prohibit such activity.* [Am. 27]

- (22) Obtaining approval from senior management for establishing business relationships need not, in all cases, imply obtaining approval from the board of directors. Granting of such approval should be possible by someone with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to make decisions affecting its risk exposure.
- (22a) *It is essential for the Union to develop a common approach and a common policy to deal with non-cooperative jurisdictions that perform poorly in combating money laundering and terrorist financing. To that end, the Member States should act on and apply directly any lists of countries published by the FATF in their national systems to combat money laundering and terrorist financing. Furthermore, the Member States and the Commission should identify other non-cooperative jurisdictions on the basis of all information available. The Commission should develop a common approach to measures to be used to protect the integrity of the internal market against those non-cooperative jurisdictions. [Am. 28]*

- (23) In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers whose identification has been carried out elsewhere to be introduced to the obliged entities. Where an obliged entity relies on a third party, the ultimate responsibility for the customer due diligence procedure remains with the obliged entity to whom the customer is introduced. The third party, or the person that has introduced the customer, should also retain his own responsibility for compliance with the requirements in this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that he has a relationship with the customer that is covered by this Directive.

- (24) In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external natural or legal persons not covered by this Directive, any anti-money laundering and anti-terrorist financing obligations for those agents or outsourcing service providers as part of the obliged entities, may arise only from contract and not from this Directive. The responsibility for complying with this Directive should remain *primarily* with the obliged entity ~~covered hereby~~. *In addition, Member States should ensure that any such third parties may be held liable for breaches of national provisions adopted pursuant to this Directive.*
- [Am. 29]

- (25) All Member States have, or should, set up ***operationally independent and autonomous*** financial intelligence units (FIUs) to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. Suspicious transactions should be reported to the FIUs, which should serve as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. This should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfiltered to FIUs, allowing them to perform their tasks properly, including international cooperation with other FIUs. ***It is important that Member States provide FIUs with the necessary resources to ensure that they have full operational capacity to deal with the current challenges posed by money laundering and terrorist financing while respecting fundamental rights, including the right to privacy and data protection.*** [Am. 30]

(26) By way of derogation from the general prohibition on executing suspicious transactions, obliged entities may execute suspicious transactions before informing the competent authorities, where refraining from the execution thereof is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

(26a) Since a huge proportion of illicit financial flows ends up in tax havens, the Union should increase the pressure it brings to bear on those countries to cooperate, in order to combat money laundering and terrorist financing. [Am. 31]

- (27) Member States should have the possibility to designate an appropriate self-regulatory body of the professions referred to in Article 2(1)(3)(a),(b), and (d) as the authority to be informed in the first instance in place of the FIU. In line with the case law of the European Court of Human Rights, a system of first instance reporting to a self-regulatory body constitutes an important safeguard to uphold the protection of fundamental rights as concerns the reporting obligations applicable to lawyers.
- (28) Where a Member State decides to make use of the exemptions provided for in Article 33(2), it may allow or require the self-regulatory body representing the persons referred to therein not to transmit to the FIU any information obtained from those persons in the circumstances referred to in that Article.

- (29) There have been a number of cases of *individuals, including* employees *and representatives* who report their suspicions of money laundering being subject to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, this is a crucial issue for the effectiveness of the anti-money laundering and anti-terrorist financing system. Member States should be aware of this problem and should do whatever they can to protect *individuals, including* employees *and representatives* from such threats or hostile action, *as well as from other adverse treatment or adverse consequences, making it easier for them to report suspicions, thereby strengthening the fight against money laundering.* [Am. 32]
- (30) Directive 95/46/EC of the European Parliament and of the Council¹, as transposed into national law, is applicable to the processing of personal data for the purposes of this Directive.

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

- (30a) *Regulation (EC) No 45/2001 of the European Parliament and of the Council¹ is applicable to the processing of personal data by the Union institutions and bodies for the purposes of this Directive. [Am. 33]*
- (31) Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. The processing of personal data should be permitted in order to comply with the obligations laid down in this Directive, including carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, *identification of a politically exposed person*, sharing of information by competent authorities and sharing of information by financial institutions *and obliged entities*. The personal data collected should be limited to what is strictly necessary for the purpose of complying with the requirements of this Directive and not further processed in a way inconsistent with Directive 95/46/EC. In particular, further processing of personal data for commercial purposes should be strictly prohibited. [Am. 34]

¹ *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).*

- (32) The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States. *The eradication of such phenomena requires a resolute political will and cooperation at all levels.* [Am. 35]
- (32a) *It is of the utmost importance that investment that is co-financed by the Union budget fulfils the highest standards in order to prevent financial crimes including corruption and tax evasion. In 2008, the EIB therefore adopted an internal guideline entitled "Policy on preventing and deterring prohibited conduct in European Investment Bank activities" with Article 325 TFEU, Article 18 of the EIB Statute and Council Regulation (EC, Euratom) No 1605/2002¹ as its legal basis. Following adoption of the policy, the EIB is to report on suspicions or alleged cases of money laundering affecting EIB supported projects, operations and transactions to the Luxembourg FIU.* [Am. 36]
- ~~(33) — This Directive is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including the provisions of Framework decision 977/2008/JHA.~~ [Am. 37]

¹ *Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities (OJ L 248, 16.9.2002, p. 1).*

- (34) The rights of access of the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to information contained in a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Limitations on that right in accordance with Article 13 of Directive 95/46/EC may therefore be justified. ***However, such limitations have to be counterbalanced by the effective powers granted to the data protection authorities, including indirect access powers, laid down in Directive 95/46/EC, enabling them to investigate, on an ex officio basis or on the basis of a complaint, any claims concerning problems with personal data processing. This should in particular include access to the data file at the obliged entity. [Am. 38]***
- (35) Persons who merely convert paper documents into electronic data and act under a contract with a credit institution or a financial institution do not fall within the scope of this Directive, nor does any natural or legal person that provides credit or financial institutions solely with a message or other support systems for transmitting funds or with clearing and settlement systems.

- (36) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Union credit or financial institutions have branches or subsidiaries located in third countries where the law in that area is deficient, they should, in order to avoid the application of very different standards within the institution or group of institutions, apply Union standards or notify the competent authorities of the home Member State if application of such standards is impossible.
- (37) Feedback should, ~~where practicable~~ **where possible**, be made available to obliged entities on the usefulness and follow-up of the suspicious transactions reports they present. To make this possible, and to be able to review the effectiveness of their systems to combat money laundering and terrorist financing Member States should keep and improve the relevant statistics. To further enhance the quality and consistency of the statistical data collected at Union level, the Commission should keep track of the Union-wide situation with respect to the fight against money laundering and terrorist financing and publish regular overviews, ***including an evaluation of national risk assessments. The Commission should carry out the first such overview within one year from the date of entry into force of this Directive.***
- [Am. 39]

- (37a) *Member States should not only ensure that obliged entities comply with the relevant rules and guidelines, but should also have systems in place that actually minimise the risks of money laundering within those entities. [Am. 40]*
- (37b) *In order to be able to review the effectiveness of their systems to combat money laundering and terrorist financing, Member States should keep and improve the relevant statistics. In order further to enhance the quality and consistency of the statistical data collected at Union level, the Commission should keep track of the Union-wide situation with respect to the fight against money laundering and terrorist financing and should publish regular overviews. [Am. 41]*
- (38) Competent authorities should ensure that, in regard to currency exchange offices, trust and company service providers or gambling service providers, the persons who effectively direct the business of such entities and the beneficial owners of such entities are fit and proper persons. The criteria for determining whether or not a person is fit and proper should, as a minimum, reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

- (39) Taking into account the transnational character of money laundering and terrorist financing, coordination and cooperation between EU FIUs are extremely important. Such cooperation has so far been addressed only by Council Decision 2000/642/JHA¹. In order to ensure better coordination and cooperation between FIUs, and in particular to ensure that suspicious transactions reports reach the FIU of the Member State where the report would be of most use, more detailed, further going and up-dated rules should be included in this Directive.
- (40) Improving the exchange of information between FIUs within the Union is of particular importance to face the transnational character of money laundering and terrorist financing. The use of secure facilities for the exchange of information, ~~especially the decentralised computer network FIU.net and the techniques offered by that network~~ *such facilities* should be encouraged by Member States. [**Am. 42**]

¹ Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (OJ L 271, 24.10.2000, p. 4).

(41) The importance of combating money laundering and terrorist financing should lead Member States to lay down effective, proportionate and dissuasive sanctions in national law for failure to respect the national provisions adopted pursuant to this Directive. Member States currently have a diverse range of administrative measures and sanctions for breaches of the key preventative measures. This diversity could be detrimental to the efforts put into combating money laundering and terrorist financing and the Union's response is at risk of being fragmented. This Directive should therefore include a range of administrative measures and sanctions that Member States shall have available for systematic breaches of the requirements relating to customer due diligence measures, record keeping, reporting of suspicious transactions and internal controls of obliged entities. That range should be sufficiently broad to allow Member States and competent authorities to take account of the differences between obliged entities, in particular between financial institutions and other obliged entities, as regards their size, characteristics, *level of risk* and areas of activity. In the application of this Directive, Member States should ensure that the imposition of administrative measures and sanctions in accordance with this Directive and of criminal sanctions in accordance with national law does not breach the principle of *ne bis in idem*. [Am. 43]

- (42) Technical standards in financial services should ensure consistent harmonisation and adequate protection of depositors, investors and consumers across the Union. As bodies with highly specialised expertise, it would be efficient and appropriate to entrust the ESAs with the elaboration of draft regulatory technical standards which do not involve policy choices, for submission to the Commission.
- (42a) To allow competent authorities and obliged entities to better evaluate the risks arising from certain transactions, the Commission should draw up a list of the jurisdictions outside the Union that have implemented rules and regulations similar to those laid down in this Directive. [Am. 44]*
- (43) The Commission should adopt the draft regulatory technical standards developed by the ESAs pursuant to Article 42 of this Directive by means of delegated acts pursuant to Article 290 TFEU and in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010.

- (44) In view of the very substantial amendments that would need to be made to Directives 2005/60/EC and 2006/70/EC, they should be merged and replaced for reasons of clarity and consistency.
- (45) Since the objective of this Directive, namely the protection of the financial system by means of prevention, investigation and detection of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States, as individual measures adopted by Member States to protect their financial systems could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Union public policy but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

- (46) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular, the respect for private and family life, the *presumption of innocence*, the right to protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, and the right of defence. [Am. 45]
- (47) In line with Article 21 of the Charter prohibiting any discrimination based on any ground, Member States have to ensure that this Directive is implemented, as regards risk assessments in the context of customer due diligence, without discrimination.

- (48) In accordance with the Joint Political Declaration of Member States and the Commission of 28 September 2011 on explanatory documents, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.
- (48a) *Member States and obliged entities, when applying this Directive or national law transposing this Directive, are bound by Council Directive 2000/43/EC¹. [Am. 46]*
- (48b) The European Data Protection Supervisor delivered an opinion on 4 July 2013²,

HAVE ADOPTED THIS DIRECTIVE:

¹ *Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (OJ L 180, 19.7.2000, p. 22).*

² *OJ C 32, 4.2.2014, p. 9.*

CHAPTER I
GENERAL PROVISIONS

Section 1

Subject-matter, scope and definitions

Article 1

1. Member States shall ensure that money laundering and terrorist financing are prohibited.
2. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:
 - (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property *or of avoiding freezing or confiscation orders* or of assisting any person who is involved in the commission of such activity to evade the legal consequences of that person's action; [Am. 47]

- (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;
 - (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;
 - (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).
3. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

4. For the purposes of this Directive, ‘terrorist financing’ means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA¹, as amended by Council Framework Decision 2008/919/JHA².
5. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 2 and 4 may be inferred from objective factual circumstances.

¹ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

² Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/474/JHA on combating terrorism (OJ L 330, 9.12.2008, p. 21).

Article 2

1. This Directive shall apply to the following obliged entities:
 - (1) credit institutions;
 - (2) financial institutions;
 - (3) the following natural or legal persons acting in the exercise of their professional activities:
 - (a) auditors, external accountants and tax advisors;
 - (b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or immovable property transaction, or by assisting in the planning or execution of transactions for their client concerning the:
 - (i) buying and selling of real property or business entities;
 - (ii) managing of client money, securities or other assets;
 - (iii) opening or management of bank, savings or securities accounts;
 - (iv) organisation of contributions necessary for the creation, operation or management of companies;
 - (v) creation, operation or management of trusts, *foundations*, *mutuals*, companies or similar structures; **[Am. 48]**

- (c) trust or company service providers not already covered under point (a) or (b);
- (d) estate agents, including letting agents, *in so far as they are involved in financial transactions*; [Am. 49]
- (e) other natural or legal persons trading in goods *or services*, only to the extent that payments are made or received in cash in an amount of EUR 7 500 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked; [Am. 50]
- (f) providers of gambling services.

With the exception of casinos, Member States may decide to exempt in full or in part certain gambling services, as referred to in point (3)(f) of the first subparagraph, from national provisions transposing this Directive on the basis of the low risk posed by the nature of the services on the basis of risk assessments. Before applying any such an exemption, the Member State concerned shall seek the approval of the Commission. [Am. 153]

2. Member States may decide that natural or legal persons that engage in a financial activity on an occasional or very limited basis where there is little risk of money laundering or terrorist financing occurring, do not fall within the scope of this Directive provided that the natural or legal person fulfils all of the following criteria:
- (a) the financial activity is limited in absolute terms;
 - (b) the financial activity is limited on a transaction basis;
 - (c) the financial activity is not the main activity;
 - (d) the financial activity is ancillary and directly related to the main activity;
 - (e) the main activity is not an activity referred to in paragraph 1, with the exception of the activity referred to in point (3)(e) of paragraph 1;
 - (f) the financial activity is provided only to the customers of the main activity and is not generally offered to the public.

The first subparagraph shall not apply to natural or legal persons engaged in the activity of money remittance within the meaning of Article 4(13) of Directive 2007/64/EC of the European Parliament and of the Council¹.

3. For the purposes of point (a) of paragraph 2, Member States shall require that the total turnover of the financial activity does not exceed a threshold, which must be sufficiently low. That threshold shall be established at national level, depending on the type of financial activity.
4. For the purposes of point (b) of paragraph 2, Member States shall apply a maximum threshold per customer and single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked. That threshold shall be established at national level, depending on the type of financial activity. It shall be sufficiently low 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.

¹ Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 5.12.2007, p. 1).

5. For the purposes of point (c) of paragraph 2, Member States shall require that the turnover of the financial activity does not exceed 5 % of the total turnover of the natural or legal person concerned.
6. In assessing the risk of money laundering or terrorist financing occurring for the purposes of this Article, Member States shall pay special attention to any financial activity which is regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.
7. Any decision pursuant to this Article shall state the reasons on which it is based. Member States shall provide for the possibility of withdrawing that decision should circumstances change.
8. Member States shall establish risk-based monitoring activities or take any other adequate measures to ensure that the exemption granted by decisions pursuant to this Article is not abused.

Article 3

For the purposes of this Directive the following definitions shall apply:

- (1) "credit institution" means a credit institution as defined in point 1 of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council¹, including branches thereof, as defined in point 17 of Article 4(1) of that Regulation, located in the Union, whether its head office is situated within the Union or in a third country;
- (2) "financial institution" means:
 - (a) an undertaking other than a credit institution the principal activity of which is to pursue one or more of the activities listed in points (2) to (12) and points (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council², including the activities of currency exchange offices (bureaux de change);
 - (b) an insurance company duly authorised in accordance with Directive 2009/138/EC of the European Parliament and of the Council³, insofar as it carries out activities covered by that Directive;

¹ 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 (OJ L 176, 27.6.2013, p. 1).

² Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

³ 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 (Solvency II) (OJ L 335, 17.12.2009, p. 1).

- (c) an investment firm as defined in point (1) of Article 4(1) of Directive 2014/65/EU of the European Parliament and of the Council¹;
 - (d) a collective investment undertaking marketing its units or shares;
 - (e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council², with the exception of intermediaries as referred to in Article 2(7) of that Directive, when they act in respect of life insurance and other investment related services;
 - (f) branches of financial institutions as referred to in points (a) to (e) that are located in the Union, whether its head office is situated in the Union or in a third country;
- (3) "property" means assets of any 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;

¹ Directive 2014/65/EU of 15 May 2014 of the European Parliament and of the Council on markets in financial instruments amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

² Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation (OJ L 9, 15.1.2003, p. 3).

- (4) "criminal activity" means any kind of criminal involvement in the commission of the following serious crimes:
- (a) acts as defined in Articles 1 to 4 of Framework Decision 2002/475/JHA, as amended by Framework Decision 2008/919/JHA;
 - (b) any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
 - (c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA¹;
 - (d) fraud affecting the Union's financial interests, at least serious, as defined in Article 1(1) and Article 2 of the Convention on the Protection of the European Communities' Financial Interests²;

¹ Council Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (OJ L 351, 29.12.1998, p. 1).

² OJ C 316, 27.11.1995, p. 49.

- (e) corruption;
- (f) all offences, including tax ~~crimes~~ **offences** related to direct taxes and indirect taxes, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months; [Am. 52; Am. does not concern all languages]

(4a) *"self-regulatory body" means a body that has the power, recognised by national law, to establish the obligations and rules governing a certain profession or a certain field of economic activity, which must be complied with by natural or legal persons in that profession or field; [Am. 53]*

(5) "beneficial owner" means any natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted and includes at least:

(a) in the case of corporate entities:

(i) the natural person who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards.

~~A percentage~~ ***In any event, a shareholding*** of 25 % plus one share shall ~~be by a natural person is~~ evidence of ownership or control through ~~shareholding and applies to every level of direct and indirect ownership;~~ ***a shareholding of 25 % plus one share in the customer, held by a corporate entity, which is under the control of a natural person, or by multiple corporate entities, which are under the control of the same natural person, shall be an indication of indirect ownership; the notion of control shall be determined, inter alia, in accordance with the criteria laid down in Article 22(1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council¹; however, this applies without prejudice to the right for Member States to decide that a lower percentage may be evidence of ownership or control;***

- (ii) if there is any doubt that the person identified in point (i) is the beneficial owner ***or if after taking all the necessary measures no person can be identified in point (i)***, the natural person who exercises control over the management of a legal entity through other means, ***which may include the senior management;***

¹ ***Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the 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 (OJ L 182, 29.6.2013, p. 19).***

(iia) where no natural person is identified under point (i) or (ii), the natural person who holds the position of senior managing official, in which case, the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under points (i) and (ii) in order to prove the inability to identify such persons;

(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts ***or mutuals***, which administer and distribute funds:

(i) the natural person who exercises control over 25 % or more of the property of a legal arrangement or entity; and

(ii) where the future beneficiaries have already been determined, the natural person who is the beneficiary of 25 % or more of the property of a legal arrangement or entity; or

(iii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates. For beneficiaries of trusts that are designated by characteristics or by class, obliged entities shall obtain sufficient information concerning the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights;

(iiiia) for trusts, the identity of the settlor, trustee, the protector (if any), the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a chain of control or ownership); [Am. 54]

- (6) "trust or company service provider" means any natural or legal person which by way of business provides any of the following services to third parties:
- (a) forming companies or other legal persons;
 - (b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
 - (c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;
 - (d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;
 - (e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Union law or subject to equivalent international standards;

- (7) (a) "foreign politically exposed persons" means natural persons who are or have been entrusted with a prominent public function by a third country;
- (b) "domestic *politically exposed* persons" means natural persons who are or who have been entrusted by ~~a~~ *the* Member State with a prominent public function; **[Am. 55; Am. does not concern all languages]**
- (c) "persons who are or who have been entrusted with a prominent function by an international organisation" means directors, deputy directors and members of the board or equivalent function of an international organisation;
- (d) "natural persons who are or have been entrusted with a prominent public function" include the following:
- (i) heads of State, heads of government, ministers and deputy or assistant ministers;
 - (ii) members of parliaments *or similar legislative bodies*; **[Am. 56]**
 - (iii) 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;

- (iv) members of courts of auditors or of the boards of central banks;
- (v) ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces;
- (vi) *senior* members of the administrative, management or supervisory bodies of State owned enterprises. [Am. 57]

None of the categories set out in points (i) to (vi) shall be understood as covering middle-ranking or more junior officials;

- (e) "family members" means:
 - (i) the spouse;
 - (ii) any partner considered to be equivalent to the spouse;
 - ~~(iii) the children and their spouses or partners; [Am. 58]~~
 - ~~(iv) the parents; [Am. 59]~~

- (f) ~~"persons known to be~~ close associates" means: **[Am. 87]**
- (i) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in points (7)(a) to (d);
 - (ii) any natural person who has ~~sole~~ beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in points (7)(a) to (d); **[Am. 60]**
- (8) "senior management" means an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to make decisions affecting its risk exposure. It need not, in all cases, involve a member of the board of directors;
- (9) "business relationship" means a business, professional or commercial relationship which is connected with the professional activities of the obliged entities and which is expected, at the time when the contact is established, to have an element of duration;

- (10) "gambling services" means any service which involves 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 a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services;
- (10a) ***"betting transaction" means all the stages in the commercial relationship between, on the one hand, the gambling service provider and, on the other, the customer and the beneficiary of the registration of the bet and the stake until the payout of any winnings; [Am. 61]***
- (11) "group" means group as defined in Article 2(12) of Directive 2002/87/EC of the European Parliament and of the Council¹;

¹ Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate and amending Council Directives 73/239/EEC, 79/267/EEC, 92/49/EEC, 92/96/EEC, 93/6/EEC and 93/22/EEC, and Directives 98/78/EC and 2000/12/EC of the European Parliament and of the Council (OJ L 35, 11.2.2003, p. 1).

(11a) "non-face-to-face", means concluding a contract or carrying out a transaction, where the contractor or intermediary and the consumer are not simultaneously physically present, by exclusive means of the internet, telemarketing or other electronic means of communication up to and including the time at which the contract is concluded or the transaction is carried out. [Am. 62]

Article 4

1. Member States shall, *in accordance with the risk-based approach*, ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the obliged entities referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes. **[Am. 63]**

2. Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

The Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing, *provided that such provisions are in full compliance with Union law, especially as regards Union data protection rules and the protection of fundamental rights as enshrined in the Charter. Such provisions shall not unduly prevent consumers from accessing financial services and shall not constitute an obstacle to the functioning of the internal market.* [Am. 64]

Section 2

Risk assessment

Article 6

1. ***The Commission shall conduct an assessment on the money laundering and terrorist financing risks affecting the internal market, with particular reference to cross-border activities. To that end, the Commission shall consult the Member States, the ESA shall provide a joint opinion on the money laundering and terrorist financing risks affecting the internal market, the European Data Protection Supervisor, the Article 29 Working Party, Europol and other relevant authorities.***

The risk assessment referred to in the first subparagraph shall cover at least the following:

- (a) the overall extent of money laundering and the areas of the internal market that are at greater risk;***
- (b) the risks associated with each relevant sector, in particular the non-financial sectors and the gambling sector;***

- (c) *the most widespread means used by criminals to launder illicit proceeds;*
- (d) *the recommendations to the competent authorities on the effective deployment of resources;*
- (e) *the role of EUR banknotes in criminal activities and money laundering.*

The risk assessment shall also include proposals for minimum standards for risk assessments to be conducted by competent national authorities. Those minimum standards shall be developed in cooperation with Member States and shall involve the industry and other relevant stakeholders through public consultations and private stakeholders meetings as appropriate.

The Commission shall issue the ~~opinion~~ *risk assessment* by ...* *and shall update it a biannual basis or more frequently if appropriate.*

* OJ please insert date: **12 months** after the date of entry into force of this Directive.

2. The Commission shall make the ~~opinion~~ ***risk assessment*** available to assist Member States and obliged entities to identify, manage and mitigate the risk of money laundering and terrorist financing, ***and to allow other stakeholders, including national legislators, the European Parliament, the ESAs, Europol and the Committee of Union FIUs, to better understand the risks. A summary of the assessment shall be publicly available. That summary shall not contain classified information.***

- 2a. ***The Commission shall submit an annual report to the European Parliament and to the Council on the findings resulting from the regular risk assessments and the action taken based on those findings. [Am. 65]***

Article 6a

1. *Without prejudice to the infringement proceedings provided for in the TFEU, the Commission shall ensure that national law to combat money laundering and terrorist financing, adopted by Member States pursuant to this Directive is implemented effectively and is consistent with the European framework.*
2. *For the application of paragraph 1, the Commission shall be assisted, where appropriate, by the ESAs, Europol, the Committee of Union FIUs, and any other competent European authority.*
3. *Assessments of national law combat money laundering and terrorist financing provided for in paragraph 1 shall be without prejudice to those conducted by the Financial Action Task Force or Moneyval. [Am. 66]*

Article 7

1. Each Member State shall take appropriate steps to identify, assess, understand and mitigate the money laundering and terrorist financing risks affecting it, *as well as any data protection concerns in that regard*, and keep the assessment up-to-date.
2. Each Member State shall designate an authority to coordinate the national response to the risks referred to in paragraph 1. The identity of that authority shall be notified to the Commission, the ESAs, *Europol* and other Member States.
3. In carrying out the assessments referred to in paragraph 1, Member States ~~may~~ *shall* make use of the ~~opinion~~ *risk assessment* referred to in Article 6(1).
4. Each Member State shall carry out the assessment referred to in paragraph 1 and:
 - (a) use the assessment(s) to improve its anti-money laundering and combating terrorist financing regime, in particular by identifying any areas where obliged entities shall apply enhanced measures and, where appropriate, specifying the measures to be taken;

- (aa) *identify, where appropriate, sectors or areas of negligible, lower or greater risk of money laundering and terrorist financing;*
- (b) use the assessment(s) to assist it in the allocation and prioritisation of resources to combat money laundering and terrorist financing;
- (ba) *use the assessment(s) to ensure that appropriate rules are drawn up for each sector or area, in accordance with the risk of money laundering;*
- (c) make appropriate information available *in a timely manner* to obliged entities *to enable them* to carry out ~~out~~ their own money laundering and terrorist financing risk assessments.

5. Member States shall make the results of their risk assessments available to the other Member States, the Commission, and the ESAs upon request. *A summary of the assessment shall be made publicly available. That summary shall not contain classified information.* [Am. 67]

Article 8

1. Member States shall ensure that obliged entities take appropriate steps to identify and assess their money laundering and terrorist financing risks taking into account risk factors including customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities.
2. The assessments referred to in paragraph 1 shall be documented, kept up to date and be made available *upon request* to competent authorities and self-regulatory bodies. **[Am. 68]**
3. Member States shall ensure that obliged entities have policies, controls and procedures to mitigate and manage effectively the money laundering and terrorist financing risks identified at Union level, Member State level, and at the level of obliged entities. Policies, controls and procedures should be proportionate to the nature and size of those obliged entities *and the risk of money laundering and terrorist financing and should respect data protection rules*. **[Am. 69]**

4. The policies and procedures referred to in paragraph 3 shall at least include:
 - (a) the development of internal policies, procedures and controls, including *model risk management practices*, customer due diligence, reporting, record keeping, internal control, compliance management (including, when appropriate to the size and nature of the business, the appointment of a compliance officer at management level) and employee screening. *Those measures shall not allow the obliged entities to ask consumers to provide more personal data than necessary; [Am. 70]*
 - (b) when appropriate with regard to the size and nature of the business, an independent audit function to test internal policies, procedures and controls referred to in point (a).
5. Member States shall require obliged entities to obtain approval from senior management for the policies and procedures they put in place, and shall monitor and enhance the measures taken, where appropriate.

Article 8a

- 1. In order to develop a common approach and common policies against non-cooperative jurisdictions with deficiencies in the field of combating money laundering, Member States shall periodically endorse and adopt the lists of countries published by the FATF.*
- 2. The Commission shall coordinate preparatory work at the Union level on the identification of third countries with grave strategic deficiencies in their money laundering systems that pose significant risks to the financial system of the Union, taking into account the criteria set out in point (3) of Annex III.*
- 3. The Commission shall be empowered to adopt delegated acts in order to establish a list of countries as defined in paragraph 2.*
- 4. The Commission shall monitor on a regular basis the evolution of the situation in the countries defined in paragraph 2 of this Article on the basis of criteria set out in point (3) of Annex III and, where appropriate, shall review the list referred to in paragraph 3 of this Article. [Am. 71]*

CHAPTER II
CUSTOMER DUE DILIGENCE

Section 1
General provisions

Article 9

Member States shall prohibit their credit and financial institutions from keeping anonymous accounts ~~or~~, anonymous passbooks *or from issuing anonymous electronic payment cards which do not meet the conditions laid down in Article 10a*. Member States shall in all cases require that the owners and beneficiaries of existing anonymous accounts ~~or~~, anonymous passbooks *or anonymous payment cards* be made the subject of customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way. [Am. 72]

Article 10

Member States shall ensure that obliged entities apply customer due diligence measures in the following cases:

- (a) when establishing a business relationship;
- (b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- (c) for natural or legal persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 7 500 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- (d) for ~~providers of gambling services~~ *casinos*, when carrying out occasional 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;

- (da) for on-line gambling when establishing the business relationship;*
- (db) for other providers of gambling services, when paying out winnings of EUR 2 000 or more; [Am. 73]*
- (e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- (f) when there are doubts about the veracity or adequacy of previously obtained customer identification data;
- (fa) when a company is established. [Am. 74]*

Article 10a

- 1. Member States may, on the basis of proven low risk, apply exemptions to obliged entities from customer due diligence with respect to electronic money as defined in Article 2(2) of Directive 2009/110/EC of the European Parliament and of the Council ¹, if the following conditions are met:**
- (a) the payment instrument is not reloadable;*
 - (b) the maximum amount stored electronically does not exceed EUR 250; Member States may increase this limit up to EUR 500 for payment instruments that can only be used in that one particular Member State;*
 - (c) the payment instrument is used exclusively to purchase goods or services;*
 - (d) the payment instrument cannot be funded with electronic money;*
 - (e) redemption in cash and cash withdrawal are forbidden unless identification and verification of the identity of the holder, adequate and appropriate policies and procedures on redemption in cash and cash withdrawal, and record keeping obligations are performed.*

¹ *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 (OJ L 267, 10.10.2009, p. 7).*

2. *Member States shall ensure that customer due diligence measures are always applied before redemption of the monetary value of the electronic money exceeding EUR 250.*

3. *This Article shall not prevent Member States from allowing obliged entities to apply simplified customer due diligence measures in respect of electronic money in accordance with Article 13 of this Directive if the conditions laid down in this Article are not met. [Am. 75]*

Article 11

1. Customer due diligence measures shall comprise:
 - (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
 - (b) ~~identifying~~ ***in addition to the identification of*** the beneficial owner ~~and listed in a register pursuant to Article 29~~, taking reasonable measures to verify the beneficial owner's identity to the satisfaction of the institution or person covered by this Directive, including, as regards legal persons, trusts, ***foundations, mutuals, holdings and all other similar existing or future*** legal arrangements, taking ~~reasonable~~ ***all necessary*** measures to understand the ownership and control structure of the customer, ***assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship***;
 - (c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, ~~where necessary,~~ the source of funds and ensuring that the documents, data or information held are kept up to date. [Am. 76]

1a. When performing the measures referred to in points (a) and (b) of paragraph 1, obliged entities shall also be required to verify that any person purporting to act on behalf of the customer is so authorised to do so and shall be required to identify and verify the identity of that person. [Am. 77]

2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis.

3. When assessing money laundering and terrorist financing risks, Member States shall require obliged entities to take into account at least the variables set out in Annex I.

4. Member States shall ensure that obliged entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.
5. For life or other investment-related insurance business, Member States shall ensure that financial institutions shall, in addition to the customer due diligence measures required for the customer and the beneficial owner, 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) for beneficiaries that are identified as specifically named natural or legal persons or legal arrangements, taking the name of the person;
 - (b) for beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

For both the cases referred to in points (a) and (b) of the first subparagraph, the verification of the identity of the beneficiaries shall occur 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, 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 own benefit the value of the policy assigned.

Article 12

1. Member States shall require that the verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying out of the transaction.
2. By way of derogation from paragraph 1, Member States may allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship *or during the execution of the transaction for entities subject to the obligations referred to in Article 2(1) and, in any event, at the time when any winnings are paid out*, 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 those procedures shall be completed as soon as practicable after the initial contact. **[Am. 78]**
3. By way of derogation from paragraphs 1 and 2, Member States may allow the opening of a bank account provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with paragraphs 1 and 2 is obtained.

4. Member States shall require that, where the institution or person concerned is unable to comply with points (a), (b) and (c) of Article 11(1), it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall consider terminating the business relationship and making a suspicious transaction report to the FIU in accordance with Article 32 in relation to the customer.

Member States shall not apply the previous subparagraph to, notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such an exemption relates to ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings.

5. Member States shall require that obliged entities apply the customer due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change.

Section 2
Simplified customer due diligence

Article 13

1. Where a Member State or an obliged entity identifies areas of lower risk, that Member State may allow obliged entities to apply simplified customer due diligence measures.
2. Before applying simplified customer due diligence measures obliged entities shall ascertain that the customer relationship or transaction presents a lower degree of risk.
3. Member States shall ensure that obliged entities carry out sufficient monitoring of the ~~transaction~~ *transactions* or business ~~relationship~~ *relationships* to enable the detection of unusual or suspicious transactions. **[Am. 79]**

Article 14

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, Member States and obliged entities shall take into account at least the factors of *relating to customer and product, service, transaction or delivery channel* as potentially lower risk situations set out in Annex II. **[Am. 80]**

Article 15

The ESAs shall, by ...*, issue guidelines addressed to competent authorities and the obliged entities referred to in Article 2(1)(1) and (2) in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010, on the risk factors to be taken into consideration and/or the measures to be taken in situations where simplified due diligence measures are appropriate. Specific account should be taken of the nature and size of the business, and where appropriate and proportionate, specific measures should be laid down. [**Am. 81**]

* OJ please insert date: **12 months** after the date of entry into force of this Directive.

Section 3

Enhanced customer due diligence

Article 16

1. In cases identified in Articles 17 to 23 of this Directive and in other cases of higher risk that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.
2. Member States shall require obliged entities to examine, ~~as far as reasonably possible,~~ the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose, *or which constitute tax offences within the meaning of Article 3(4)(f)*. In particular, they 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. *Where an obliged entity determines such an unusual or suspicious transaction or activity, it shall, without delay, inform the FIUs of all Member States that might be concerned.* [Am. 82]

3. When assessing the money laundering and terrorist financing risks, Member States and obliged entities shall take into account at least the factors ~~of~~ *relating to customer and product, service, transaction or delivery channel as* potentially higher-risk situations set out in Annex III. [Am. 83]

4. The ESAs shall, by ...^{*}, issue guidelines addressed to competent authorities and the obliged entities referred to Article 2(1)(1) and (2) in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 on the risk factors to be taken into consideration and/or the measures to be taken in situations where enhanced due diligence measures need to be applied. [Am. 84]

^{*} OJ please insert date: *12 months* after the date of entry into force of this Directive.

Article 17

In respect of cross-border correspondent banking relationships with respondent institutions from third countries, Member States shall, in addition to the customer due diligence measures as set out in Article 11, require their credit institutions to:

- (a) gather sufficient information about a 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;
- (b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls;
- (c) obtain approval from senior management before establishing new correspondent banking relationships;
- (d) document the respective responsibilities of each institution;
- (e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

Article 18

In respect of transactions or business relationships with foreign politically exposed persons, Member States shall, in addition to the customer due diligence measures set out in Article 11, require obliged entities to:

- (a) have appropriate risk-based procedures to determine whether the customer or the beneficial owner of the customer is such a person;
- (b) obtain senior management approval for establishing or continuing business relationships with such customers;
- (c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;
- (d) conduct enhanced ongoing monitoring of the business relationship.

Article 19

In respect of transactions or business relationships with domestic politically exposed persons or persons who are or who have been entrusted with a prominent function by an international organisation, Member States shall, in addition to the customer due diligence measures set out in Article 11, require obliged entities:

- (a) to have appropriate risk-based procedures to determine whether the customer or the beneficial owner of the customer is such a person;
- (b) in cases of higher risk business relationships with such persons, to apply the measures referred to in points (b), (c) and (d) of Article 18.

Article 19a

The Commission, in cooperation with Member States and international organisations, shall draw a list of domestic politically exposed persons and persons resident in a Member State who are or who have been entrusted with a prominent function by an international organisation. The list shall be accessible by competent authorities and by obliged entities.

The Commission shall notify the persons concerned that they have been placed on or removed from the list.

The requirements in this Article shall not exempt obliged entities from their customer due diligence obligations, and obliged entities shall not rely exclusively on that information as sufficient to fulfil those obligations.

Member States shall take all appropriate measures to prevent the trade of information for commercial purposes on foreign politically exposed persons, domestic politically exposed persons, or persons who are or who have been entrusted with a prominent function by an international organisation. [Am. 85]

Article 20

Obligated entities shall take reasonable measures, *in accordance with the risk-based approach*, to determine whether the beneficiaries of a life or other investment related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. Those measures shall be taken at the latest 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 taking normal customer due diligence measures, Member States shall require obligated entities to: **[Am. 86]**

- (a) inform senior management before the payout of the policy proceeds;
- (b) conduct enhanced scrutiny on the whole business relationship with the policyholder.

Article 21

The measures referred to in Articles 18, 19 and 20, *but not those referred to in Article 19a*, shall also apply to family members or persons ~~known to be~~ *who, as indicated by evidence, are* close associates of such foreign or domestic politically exposed persons. **[Am. 87]**

Article 22

Where a person referred to in Articles 18, 19 and 20 has ceased to be *a foreign politically exposed person, a domestic politically exposed person* or a person who is or who has been entrusted with a prominent function by an international organisation, obliged entities shall be required to consider the continuing risk posed by that person and to apply such appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk. That period of time shall not be less than ~~18~~ **12** months. [**Am. 88**]

Article 23

1. Member States shall prohibit credit institutions from entering into or continuing a correspondent banking relationship with a shell bank and shall require that credit institutions take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.
2. For the purposes of paragraph 1, "shell bank" shall mean a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Section 4

Performance by third parties

Article 24

Member States may permit the obliged entities to rely on third parties to meet the requirements laid down in Article 11(1)(a), (b) and (c). However, the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party. ***In addition, Member States shall ensure that any such third parties may also be held liable for breaches of national provisions adopted pursuant to this Directive. [Am. 89]***

Article 25

1. For the purposes of this Section, "third parties" shall mean:
 - (a) obliged entities who are listed in Article 2; *or*
 - (b) other institutions and persons situated in Member States or a third country, who apply customer due diligence requirements and record keeping requirements equivalent to those laid down in this Directive and their compliance with the requirements of this Directive is supervised in accordance with Section 2 of Chapter VI.

2. The ~~Member States~~ **Commission** shall consider information available on the level of geographical risk when deciding if a third country meets the conditions laid down in paragraph 1 and shall inform ~~each other~~, the ~~Commission~~ **Member States, the obliged entities** and the ESAs to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010, of cases where they consider that a third country meets such conditions.

- 2a. *The Commission shall provide a list of jurisdictions having anti-money laundering measures equivalent to provisions of this Directive and other related rules and regulations of the Union.***
- 2b. *The list referred to in paragraph 2a shall be regularly reviewed and updated according to the information received from Member States pursuant to paragraph 2. [Am. 90]***

Article 26

1. Member States shall ensure that obliged entities obtain from the third party being relied upon the necessary information concerning the requirements laid down in Article 11(1)(a), (b) and (c).
2. Member States shall ensure that obliged entities to which the customer is being referred take adequate steps to ensure that relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner are immediately forwarded, on request, by the third party.

Article 27

1. Member States shall ensure that the home competent authority (for group-wide policies and controls) and the host competent authority (for branches and subsidiaries) may consider that an obliged entity applies the measures contained in Article 25(1) and Article 26 through its group programme, where the following conditions are met:
 - (a) an obliged entity relies on information provided by a third party that is part of the same group;
 - (b) that group applies customer due diligence measures, rules on record keeping and programmes against money laundering and terrorist financing in accordance with this Directive or equivalent rules;
 - (c) the effective implementation of requirements referred to in point (b) is supervised at group level by a *home* competent authority ***in cooperation with host competent authorities***. [Am. 91]

1a. The ESAs shall, by ...*, issue guidelines on the implementation of the supervisory regime by the competent authorities in the relevant Member States for group entities to ensure coherent and effective group level supervision. [Am. 92]

Article 28

This Section 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 obliged entity.

* ***OJ please insert date: 12 months after the date of entry into force of this Directive.***

CHAPTER III
BENEFICIAL OWNERSHIP INFORMATION

Article 29

1. Member States shall ensure that ~~corporate or~~ ***companies and other entities having legal personality, including trusts or entities with a similar structure or function to trusts, foundations, holdings and all other similar, in terms of structure or function, existing or future legal arrangements established or incorporated*** within their territory, ***or governed under their law*** obtain ~~and~~, hold ***and transmit to a public central register, commercial register or companies register within their territory*** adequate, accurate ~~and~~, current ***and up-to-date*** information on ***them and on*** their beneficial ownership, ***at the moment of establishment as well as any changes thereof.***

1a. The register shall contain the minimum information to clearly identify the company and its beneficial owner, namely the name, number, legal form and status of the entity, proof of incorporation, address of the registered office (and of the principal place of business if different from the registered office), the basic regulatory powers (such as those contained in the Memorandum and Articles of Association), the list of directors (including their nationality and date of birth) and shareholder/beneficial owner information, such as the names, dates of birth, nationality or jurisdiction of incorporation, contact details, number of shares, categories of shares (including the nature of the associated voting rights) and proportion of shareholding or control, if applicable.

The requirements stipulated in this Article shall not exempt obliged entities from their customer due diligence obligations, and obliged entities shall not rely exclusively on that information as sufficient to fulfil those obligations.

1b. Regarding trusts or other types of legal entities and arrangements, existing or future, with a similar structure or function, the information shall include the identity of the settlor, of the trustee(s), of the protector (if relevant), of the beneficiaries or class of beneficiaries, and of any other natural person exercising effective control over the trust. Member States shall ensure that trustees disclose their status to obliged entities when, as a trustee, the trustee forms a business relationship or carries out an occasional transaction above the threshold set out in points (b), (c) and (d) of Article 10. The information held should include the date of birth and nationality of all individuals. Member States shall follow the risk-based approach when publishing the trust deed and letter of wishes and shall ensure where applicable and while respecting the protection of personal information that information is disclosed to competent authorities, in particular to FIUs, and to obliged entities.

2. ~~Member States shall ensure that~~ The information referred to in ~~paragraph~~ **paragraphs 1, 1a and 1b** ~~can be accessed~~ **shall be accessible by competent authorities, in particular by FIUs, and by obliged entities of all Member States** in a timely manner ~~by competent authorities and by obliged entities~~. **Member States shall make the registers referred to in paragraph 1 publicly available following prior identification of the person wishing to access the information through basic online registration. The information shall be available online to all persons in an open and secure data format, in line with data protection rules, in particular as regards the effective protection of the rights of the data subject to access personal data and the rectification or deletion of inaccurate data. The fees charged for obtaining the information shall not exceed the administrative costs thereof. Any changes to the information displayed shall be clearly indicated in the register without delay and in any event within 30 days.**

The company registers referred to in paragraph 1 of this Article shall be interconnected by means of the European platform, the portal and optional access points established by the Member States pursuant to Directive 2012/17/EU. Member States, with the support of the Commission, shall ensure that their registers are interoperable within the system of register networking through the European platform.

2a. *The Commission, in cooperation with Member States, shall rapidly, constructively and effectively seek cooperation with third countries to encourage that equivalent central registers containing beneficial ownership information are established and information referred to in paragraphs 1 and 1a of this Article in their countries is made publically accessible.*

Priority shall be given to third countries that host a significant number of corporate or legal entities, including trusts, foundations, holdings and all other bodies that are similar in terms of structure or function and that hold shares indicating direct ownership pursuant to Article 3(5) in corporate or legal entities established in the Union.

2b. *Member States shall lay down the rules on effective, proportionate and dissuasive penalties for natural or legal persons applicable to infringements of the national provisions adopted pursuant to this Article and shall take all measures necessary to ensure that such penalties are applied. For the purposes of this Article, Member States shall establish effective anti-abuse measures with view to preventing misuse based on bearer shares and bearer share warrants.*

2c. *The Commission shall, by ...*, submit to the European Parliament and to the Council a report on the application and mode of functioning of the requirements pursuant to this Article, if appropriate, accompanied, where appropriate by a legislative proposal. [Am. 93]*

* *OJ please insert date: 3 years after the date of entry into force of this Directive.*

Article 30

- ~~1. Member States shall ensure that trustees of any express trust governed under their law obtain and hold adequate, accurate and current information on beneficial ownership regarding the trust. This information shall include the identity of the settlor, of the trustee(s), of the protector (if relevant), of the beneficiaries or class of beneficiaries, and of any other natural person exercising effective control over the trust.~~
- ~~2. Member States shall ensure that trustees disclose their status to obliged entities when, as a trustee, the trustee forms a business relationship or carries out an occasional transaction above the threshold set out in points (b), (c) and (d) of Article 10.~~
- ~~3. Member States shall ensure that the information referred to in paragraph 1 of this Article can be accessed in a timely manner by competent authorities and by obliged entities.~~
- ~~4. Member States shall ensure that measures corresponding to those in paragraphs 1, 2 and 3 apply to other types of legal entity and arrangement with a similar structure and function to trusts. [Am. 94]~~

CHAPTER IV
REPORTING OBLIGATIONS

Section 1
General provisions

Article 31

1. Each Member State shall establish an FIU in order to prevent, detect and investigate money laundering and terrorist financing.
 - 1a. The persons referred to in Article 2(1)(3)(a), (b), and (d), shall inform the FIU and/or the appropriate self-regulatory body of the profession concerned, as referred to in Article 33(1), if they suspect, or have reasonable grounds to suspect that their services are being misused for the purpose of criminal activity. [Am. 95]*
2. Member States shall notify the Commission in writing of the name and address of the respective FIUs.

3. The FIU shall be established as a *an operationally independent and autonomous* central national unit. It shall be responsible for receiving ~~(and to the extent permitted, requesting)~~, analysing and *suspicious transaction reports and other information relevant to potential money laundering, associated predicate offences or potential terrorist financing. The FIU shall be responsible for disseminating the results of its analysis to the all* competent authorities ~~disclosures of information which concern potential~~ *where there are grounds to suspect* money laundering or associated predicate offences, ~~potential~~ *or* terrorist financing ~~or are required by national legislation or regulation. It shall be able to obtain relevant additional information from obliged entities for those purposes.~~ The FIU shall be provided with adequate *financial, technical and human* resources in order to fulfil its tasks. *Member States shall ensure that the FIU is free from undue interference.* [Am. 96]

4. Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks. In addition, FIUs shall respond to requests for information by law enforcement authorities in their Member State unless there are factual reasons to assume that the provision of such information would have a negative impact on ongoing investigations or analyses, or, in exceptional circumstances, where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested. ***When the FIU receives such a request, the decision to conduct analysis or dissemination of information to the requesting law enforcement authority should remain within the FIU. Member States shall require law enforcement authorities to provide feedback to the FIU about the use made of the information provided. [Am. 97]***

5. Member States shall ensure that the FIU is empowered to take urgent action, either directly or indirectly, when there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction going ahead in order to analyse the transaction and confirm the suspicion.
6. The FIU's analysis function shall consist of an operational analysis which focusses on individual cases and specific targets and a strategic analysis addressing money laundering and terrorist financing trends and patterns.

Article 32

1. Member States shall require obliged entities, and where applicable their directors and employees, to cooperate fully by promptly:
 - (a) informing the FIU, on their own initiative, where the institution or person covered by this Directive knows, suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing and by promptly responding to requests by the FIU for additional information in such cases;
 - (b) providing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable law.
2. The information referred to in paragraph 1 of this Article shall be forwarded to the FIU of the Member State in whose territory the institution or person forwarding the information is situated *and to the FIU of the Member State where the obliged entity is established*. The person or persons designated in accordance with Article 8(4) shall forward the information. [**Am. 98**]

Article 33

1. By way of derogation from Article 32(1), Member States may, in the case of the persons referred to in Article 2(1)(3)(a), (b), ~~and~~ (d) **and (e) and those professions and categories of undertaking referred to in Article 4**, designate an appropriate self-regulatory body of the profession concerned as the authority to receive the information referred to in Article 32(1).

In all circumstances, Member States shall provide for the means and manner by which to achieve the protection of professional secrecy, confidentiality and privacy.

[Am. 99]

Without prejudice to paragraph 2, the designated self-regulatory body shall in cases referred to in the first subparagraph forward the information to the FIU promptly and unfiltered.

2. Member States shall not apply the obligations laid down in Article 32(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such an exemption relates to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 34

1. Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with Article 32(1)(a).

In accordance with national law, instructions may be given not to carry out the transaction.

2. Where such a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such a manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the obliged entities concerned shall inform the FIU immediately afterwards.

Article 35

1. Member States shall ensure that if, in the course of inspections carried out in the obliged entities by the competent authorities referred to in Article 45, or in any other way, those authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU.
2. Member States shall ensure that supervisory bodies empowered by law or regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 36

Disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity in accordance with Articles 32 and 33 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind.

Article 37

Member States shall ~~take all appropriate measures in order to protect employees~~ ***ensure that individuals, including employees and representatives*** of the obliged entity who report suspicions of money laundering or terrorist financing either internally or to the FIU ***are duly protected*** from being exposed to threats or hostile action, ***adverse treatment and adverse consequences, and in particular from adverse or discriminatory employment actions.*** ***Member States shall guarantee legal aid free of charge for such persons and shall provide secure communication channels for persons to report their suspicions of money laundering or terrorist financing. Such channels shall ensure that the identity of persons providing information is known only to the ESAs or to the FIU. Member States shall ensure that there are adequate witness protection programmes.*** [Am. 100]

Section 2
Prohibition of disclosure

Article 38

1. Obligated entities and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Articles 32 and 33 or that a money laundering or terrorist financing investigation is being or may be carried out.
2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities of Member States, including the self-regulatory bodies, *data protection authorities* or disclosure for law enforcement purposes. [**Am. 101**]
3. The prohibition laid down in paragraph 1 shall not prevent disclosure between institutions from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive provided that they belong to the same group.

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between persons referred to in Article 2(1)(3)(a) and (b) from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not, within the same legal person or a network.

For the purposes of the first subparagraph, a "network" shall mean the larger structure to which the person belongs and which shares common ownership, management, *standards, methods* or compliance control. [Am. 102]

5. For entities or persons referred to in Article 2(1)(1), (2) and (3)(a) and (b) in cases related to the same customer and the same transaction involving two or more institutions or persons, the prohibition laid down in paragraph 1 of this Article shall not prevent disclosure between the relevant institutions or persons provided that they are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in this Directive, and that they are from the same professional category and are subject to obligations as regards professional secrecy and personal data protection.

- 5a. For the purposes of this Article, third-country requirements equivalent to those laid down in this Directive shall include data protection rules. [Am. 103]*
6. Where the persons referred to in Article 2(1)(3)(a) and (b) seek to dissuade a client from engaging in illegal activity, this shall not constitute disclosure within the meaning of paragraph 1.

CHAPTER V

DATA PROTECTION, RECORD KEEPING AND STATISTICAL DATA [Am. 104]

Article 39

- 1.** Member States shall require obliged entities to store the following documents and information in accordance with national law for the purpose of the prevention, detection and investigation of possible money laundering or terrorist financing by the FIU or by other competent authorities:
 - (a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of five years after the business relationship with their customer has ended ***or after the date of the occasional transaction***. Upon expiration of that retention period, personal data shall be deleted unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention only if necessary for the prevention, detection or investigation of money laundering and terrorist financing ***and if the extension of the data retention period is justified on a case-by-case basis***. The maximum ***extension of the*** retention period ~~after the business relationship has ended shall not exceed ten~~ ***is five additional*** years;

(b) in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national law for a period of five years following either the carrying-out of the transactions or the end of the business relationship, whichever period is the shorter. Upon expiry of that retention period, personal data shall be deleted, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention only if necessary for the prevention, detection or investigation of money laundering and terrorist financing ***and if the extension of the data retention period is justified on a case by case basis.*** The maximum ***extension of the*** retention period following either the carrying-out of the transactions or the end of the business relationship, whichever period ends first, shall not exceed ~~ten~~ ***is five additional*** years.

2. ***Any personal data retained shall not be used for any purpose other than the purpose for which it has been retained, and under no circumstances shall it be used for commercial purposes. [Am. 105]***

Article 39a

- 1. With regard to the processing of personal data carried out by Member States within the framework of this Directive, the provisions of Directive 95/46/EC apply. With regard to the processing of personal data by the ESAs, the provisions of Regulation (EC) No 45/2001 apply. The collection, processing and transfer of information for anti-money laundering purposes shall be considered as a public interest under those legal acts.*
- 2. Personal data shall be processed on the basis of this Directive for the sole purpose of the prevention of money laundering and terrorist financing. Obligated entities shall inform new clients of the possible use of the personal data for money laundering prevention purposes before establishing a business relationship. Processing sensitive categories of data shall be done in accordance with Directive 95/46/EC.*
- 3. The processing of data collected on the basis of this Directive for commercial purposes shall be prohibited.*

4. *The affected person to whom disclosure of information on processing his or her data is denied by an obliged entity or competent authority, shall have the right to request through his or her data protection authority any verifications of, access and corrections to or erasure of his or her personal data, as well as the right to lodge a judicial procedure.*
5. *Access by the person concerned to information contained in a suspicious transaction report shall be prohibited. The prohibition laid down in this paragraph shall not include disclosure to the data protection authorities.*
6. *Member States shall require the obliged entities and competent authorities to recognise and comply with the effective powers of data protection authorities in accordance with Directive 95/46/EC as regards the security of the processing and accuracy of personal data, on an ex officio basis or on the basis of a complaint by the person concerned. [Am. 106]*

Article 40

- 1. *Member States shall have national centralised mechanisms enabling them to identify, in a timely manner, whether natural or legal persons hold or control bank accounts kept by financial institutions on their territory.*
- 1a. *Member States shall also have mechanisms providing the competent authorities with a means of identifying property without giving prior notice to the owner.*
- 1. Member States shall require that their obliged entities have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, in accordance with their national law, 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 manner that ensures full confidentiality of the enquiries.***
[Am. 107]

Article 40a

The collection, processing and transfer of information for anti-money laundering purposes shall be considered to be a matter of public interest under Directive 95/46/EC. [Am. 108]

Article 41

1. Member States shall, for the purposes of the preparation of national risk assessments pursuant to Article 7, ensure that they are able to review the effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems.
2. Statistics referred to in paragraph 1 shall include:
 - (a) data measuring the size and importance of the different sectors which fall under the scope of this Directive, including the number of entities and persons and the economic importance of each sector;

(b) data measuring the reporting, investigation and judicial phases of the national anti-money laundering and terrorist financing regime, including the number of suspicious transaction reports made to the FIU, the follow-up given to those reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and the value in euro of property that has been frozen, seized or confiscated;

(ba) data identifying the number and percentage of reports resulting in further investigation, with annual report to obliged institutions detailing the usefulness and follow-up of the reports they presented; [Am. 109]

(bb) data regarding the number of cross-border requests for information that were made, received, refused and partially or fully answered by the FIU. [Am. 110]

3. Member States shall ensure that a consolidated review of their statistical reports is published and shall transmit to the Commission the statistics referred to in paragraph 2.

CHAPTER VI
POLICIES, PROCEDURES AND SUPERVISION

Section 1

Internal procedures, training and feedback

Article 42

1. Member States shall require obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for anti-money laundering and combating terrorist financing purposes. Those policies and procedures shall be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries.

2. Member States shall ensure that where obliged entities have branches or majority-owned subsidiaries located in third countries where the minimum anti-money laundering and combating terrorist financing requirements are less strict than those of the Member State, their branches and majority-owned subsidiaries located in the third country implement the requirements of the Member State, including data protection, to the extent that the third country's laws and regulations so allow.
3. The Member States and the ESAs shall inform each other of cases where the third-country law does not permit application of the measures required under paragraph 1 and coordinated action could be taken to pursue a solution.
4. Member States shall require that, where third-country law does not permit application of the measures required under the first subparagraph of paragraph 1, obliged entities take additional measures to effectively handle the risk of money laundering or terrorist financing, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country shall consider additional supervisory actions, including, as appropriate, requesting the financial group to close down its operations in the host country.

5. The ESAs shall develop draft regulatory technical standards specifying the type of additional measures referred to in paragraph 4 of this Article and the minimum action to be taken by obliged entities referred to Article 2(1)(1) and (2) where third-country law does not permit application of the measures required under paragraphs 1 and 2 of this Article.

The ESAs shall submit those draft regulatory technical standards to the Commission by ... * [Am. 111]

6. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 5 in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010.
7. Member States shall ensure that sharing of information within the group is allowed provided that it does not prejudice investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law.

* OJ please insert date: ~~two years~~ **18 months after** the date of entry into force of this Directive.

8. Member States may require electronic money issuers as defined in Article 2(3) of Directive 2009/110/EC and payment providers as defined in Article 4(9) of Directive 2007/64/EC established on their territory, and whose head office is situated in another Member State or outside the Union, to appoint a central contact point in their territory to oversee the compliance with anti-money laundering and terrorist financing rules.
9. The ESAs shall develop draft regulatory technical standards on the criteria for determining the circumstances when the appointment of a central contact point pursuant to paragraph 8 is appropriate, and what the functions of the central contact points should be.

The ESAs shall submit those draft regulatory technical standards to the Commission by ...*.
10. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 9 in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010.

* OJ please insert date: two years after the date of entry into force of this Directive.

Article 43

1. Member States shall require that obliged entities take measures proportionate to their risks, nature and size so that their relevant employees are aware of the provisions adopted pursuant to this Directive, including relevant data protection requirements.

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

Where a natural person falling within any of the categories listed in Article 2(1)(3) performs 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.

2. Member States shall ensure that obliged entities have access to up-to-date information on the practices of money launderers and terrorist financiers and on indications leading to the recognition of suspicious transactions.
3. Member States shall ensure that, where practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided *to obliged entities*. [Am. 112]

- 3a. *Member States shall require that obliged entities appoint the member(s) of the management board who are responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this Directive.*
[Am. 113]

Section 2

Supervision

Article 44

1. Member States shall provide that currency exchange offices and trust or company service providers be licensed or registered and providers of gambling services be authorised.
2. In respect of the entities referred to in paragraph 1, Member States shall require competent authorities to ensure that the persons who effectively direct or will direct the business of such entities or the beneficial owners of such entities are fit and proper persons.
3. In respect of the obliged entities referred to in point (3)(a), (b), (d) and (e) of Article 2(1), Member States shall ensure that competent authorities *and self-regulatory bodies* take the necessary measures to prevent *convicted* criminals *in those areas* or their associates from holding or being the beneficial owner of a significant or controlling interest, or holding a management function in those obliged entities.
[Am. 114]

Article 45

1. Member States shall require the competent authorities to effectively monitor and to take the necessary measures with a view to ensure compliance with the requirements of this Directive.
2. Member States shall ensure that the competent authorities have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate financial, human and technical resources to perform their functions. Member States shall ensure that staff of those authorities maintain high professional standards, including standards of confidentiality and data protection, they shall be of high integrity and be appropriately skilled.
3. In the case of credit and financial institutions and providers of gambling services, competent authorities shall have enhanced supervisory powers, notably the possibility to conduct on-site inspections. ***Competent authorities in charge of supervising credit and financial institutions shall monitor the adequacy of the legal advice they receive with a view to reducing legal and regulatory arbitrage in the case of aggressive tax planning and avoidance.*** [Am. 115]

4. Member States shall ~~ensure~~ **require** that obliged entities that operate branches or subsidiaries in other Member States respect the national provisions of that other Member State pertaining to this Directive. **[Am. 116]**
5. Member States shall ensure that the competent authorities of the Member State in which the branch or subsidiary is established shall cooperate with the competent authorities of the Member State in which the obliged entity has its head office, to ensure effective supervision of the requirements of this Directive.
6. Member States shall ensure that ~~competent authorities that apply a risk-sensitive~~ **when applying a risk-based** approach to supervision, **competent authorities:**
[Am. 117]
 - (a) have a clear understanding of the money laundering and terrorist financing risks present in their country;
 - (b) have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the obliged entities; and
 - (c) base the frequency and intensity of on-site and off-site supervision on the risk profile of the obliged entity, and on the money laundering and terrorist financing risks present in the country.

7. The assessment of the money laundering and terrorist financing risk profile of obliged entities, including the risks of non-compliance, shall be reviewed both periodically and when there are major events or developments in the management and operations of the obliged entity.
8. Member States shall ensure that competent authorities take into account the degree of discretion allowed to the obliged entity, and appropriately review the risk assessments underlying this discretion, and the adequacy and implementation of its policies, internal controls and procedures.
9. In the case of the obliged entities referred to in Article 2(1)(3)(a), (b) and (d) Member States may allow the functions referred to in paragraph 1 to be performed by self-regulatory bodies, provided that they comply with paragraph 2 of this Article.
10. The ESAs shall, by ...*, issue guidelines addressed to competent authorities in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010 on the factors to be applied when conducting supervision on a risk-sensitive basis. Specific account should be taken of the nature and size of the business, and where appropriate and proportionate, specific measures should be laid down.

* OJ please insert date: 2 years after the date of entry into force of this Directive.

Section 3
Cooperation

Subsection I
National cooperation

Article 46

Member States shall ensure that policy makers, the FIU, law enforcement authorities, supervisors, *data protection authorities* and other competent authorities involved in anti-money laundering and combating terrorist financing have effective mechanisms to enable them to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

[Am. 118]

Subsection II
Cooperation with the ESAs

Article 47

Without prejudice to data protection rules, the competent authorities shall provide the ESAs with all the *relevant* information necessary to carry out their duties under this Directive.

[Am. 119]

Subsection III

Cooperation between the Commission and the FIUs Article 48

The Commission ~~may~~ **shall** lend such assistance as may be needed to facilitate coordination, including the exchange of information between Member State FIUs within the Union. It ~~may~~ **shall** regularly convene meetings ~~with~~ **of the EU FIUs' Platform composed of** representatives from Member States FIUs **and, where appropriate, meetings of the EU FIUs' Platform with EBA, EIOPA or ESMA. The EU FIUs' Platform has been set up to formulate guidance on implementation issues relevant for FIUs and reporting entities, to facilitate co-operation and to exchange views on co-operation related issues the FIUs' activities, particularly those concerning international cooperation and joint analysis, to share information on trends and risk factors in the internal market, and to ensure the participation of the FIUs in the governance of the FIU.net system. [Am. 120]**

Article 49

Member States shall ensure that their FIUs cooperate with each other *and with third-country FIUs* to the greatest extent possible irrespective of whether they are administrative, law enforcement or judicial or hybrid authorities, *without prejudice to Union data protection rules*. [Am. 121]

Article 50

1. Member States shall ensure that FIUs exchange, ~~spontaneously~~ *with other Member State FIUs and with third-country FIUs, automatically* or upon request, any information that may be relevant for the processing or analysis of information or investigation by the FIU regarding financial transactions related to money laundering or terrorist financing and the natural or legal person involved. A request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used. [Am. 122]

2. Member States shall ensure that the FIU to which the request is made is required to use the whole range of its powers which it has domestically available for receiving and analysing information when it replies to a request for information referred to in paragraph 1 from another FIU ~~based in the Union~~. The FIU to whom the request is made shall respond in a timely manner and both the requesting and requested FIU shall use secure digital means to exchange information, where possible. **[Am. 123]**

In particular, when a Member State FIU seeks to obtain additional information from an obliged entity of another Member State which operates on its territory, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is situated. That FIU shall transfer requests and answers promptly and without any filter. [Am. 124]

3. An FIU may refuse to disclose information which could lead to impairment of a criminal investigation being conducted in the requested Member State or, in exceptional circumstances, where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State or irrelevant to the purposes for which it has been collected. Any such refusal shall be appropriately justified to the FIU requesting the information.

Article 51

Information and documents received pursuant to Articles 49 and 50 shall be used for the accomplishment of the FIU's tasks as laid down in this Directive. When transmitting information and documents pursuant to Articles 49 and 50, the transmitting FIU may impose restrictions and conditions for the use of that information. The receiving FIU shall comply with those restrictions and conditions. This does not affect the use for criminal investigations and prosecutions linked to the FIU's tasks to prevent, detect and investigate money laundering and terrorist financing.

Article 52

Member States shall ensure that FIUs undertake all necessary measures, including security measures, to ensure that information submitted pursuant to Articles 49 and 50 is not accessible by any other authority, agency or department, unless prior approval is given by the FIU providing the information.

Article 53

1. Member States shall ~~encourage~~ **require** their FIUs to use protected channels of communication between FIUs and to use the decentralised computer network FIU.net **themselves**. [Am. 125]
2. Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs cooperate **among themselves and, within its mandate, with Europol**, to apply sophisticated technologies. Those technologies shall allow FIUs to match their data with other FIUs in an anonymous way by ensuring full protection of personal data with the aim to detect subjects of the FIU's interests in other Member States and identify their proceeds and funds. [Am. 126]

Article 54

Member States shall ~~ensure that~~ **encourage** their FIUs **to** cooperate with Europol regarding analyses **of ongoing cases** carried out having a cross-border dimension concerning at least two Member States. [Am. 127]

Article 54a

The Commission should increase the pressure that it brings to bear on the tax havens to improve their cooperation and exchange of information in order to combat money laundering and terrorist financing. [Am. 128]

Section 4

Sanctions

Article 55

1. Member States shall ensure that obliged entities can be held liable for breaches of the national provisions adopted pursuant to this Directive. ***The penalties shall be effective, proportionate and dissuasive. [Am. 129]***
2. Without prejudice to the right of Member States to impose criminal penalties, Member States shall ensure that competent authorities may take appropriate administrative measures and impose administrative sanctions where obliged entities breach the national provisions, adopted in the implementation of this Directive, and shall ensure that they are applied. Those measures and sanctions shall be effective, proportionate and dissuasive.

3. Member States shall ensure that where obligations apply to legal persons, sanctions can be applied to the members of the management body or to any other individuals who under national law are responsible for the breach.
4. Member States shall ensure that the competent authorities have all the investigatory powers that are necessary for the exercise of their functions. In the exercise of their sanctioning powers, competent authorities shall cooperate closely to ensure that administrative measures or sanctions produce the desired results and coordinate their action when dealing with cross border cases.

Article 56

1. This Article shall at least apply to situations where obliged entities demonstrate systematic failings in relation to the requirements laid down in:
 - (a) Articles 9 to 23 (customer due diligence);
 - (b) Articles 32, 33 and 34 (suspicious transaction reporting);
 - (c) Article 39 (record keeping); and
 - (d) Articles 42 and 43 (internal controls).

2. Member States shall ensure that in the cases referred to in paragraph 1, the administrative measures and sanctions that can be applied include at least the following:
 - (a) a public statement which indicates the natural or legal person and the nature of the breach, *if necessary and proportionate after a case-by-case evaluation*; **[Am. 130]**
 - (b) an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct;
 - (c) in the case of an obliged entity subject to an authorisation, withdrawal of the authorisation;

- (d) a temporary ban against any member of the obliged entity's management body, who is held responsible, to exercise functions in institutions;
- (e) in the case of a legal person, administrative pecuniary sanctions of up to 10% of the total annual turnover of that legal person in the preceding business year;
- (f) in the case of a natural person, administrative pecuniary sanctions of up to EUR 5 000 000, or in the Member States where the euro is not the official currency, the corresponding value in the national currency on ...* [OJ please insert the date of entry into force of this Directive];
- (g) administrative pecuniary sanctions of up to twice the amount of the profits gained or losses avoided because of the breach where those can be determined.

For the purpose of point (e) of the first subparagraph, where the legal person is a subsidiary of a parent undertaking, the relevant total annual turnover shall be the total annual turnover resulting from the ~~consolidated~~ account of the ~~ultimate parent undertaking in the preceding business year~~ *subsidiary*. [Am. 131]

Article 57

1. Member States shall ensure that competent authorities publish any sanction or measure imposed for breach of the national provisions adopted in the implementation of this Directive, *if necessary and proportionate after a case-by-case evaluation*, without undue delay including information on the type and nature of the breach and the identity of persons responsible for it, ~~unless such publication would seriously jeopardise the stability of financial markets~~. Where publication would cause a disproportionate damage to the parties involved, competent authorities ~~shall~~ *may* publish the sanctions on an anonymous basis. [Am. 132]

2. Member States shall ensure that when determining the type of administrative sanctions or measures and the level of administrative pecuniary sanctions, the competent authorities shall take into account all relevant circumstances, including:
- (a) the gravity and the duration of the breach;
 - (b) the degree of responsibility of the natural or legal person responsible;
 - (c) the financial strength of the natural or legal person responsible as indicated by the total turnover of that person or the annual income of that person;
 - (d) the importance of profits gained or losses avoided by the natural or legal person 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 level of cooperation of the natural or legal person responsible with the competent authority;
 - (g) previous breaches by the natural or legal person responsible.

3. *In order to ensure their consistent application and dissuasive effect across the Union*, the ESAs shall, by ...^{*} issue guidelines addressed to competent authorities in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010 on types of administrative measures and sanctions and level of administrative pecuniary sanctions applicable to obliged entities referred to in Article 2(1)(1) and (2). [**Am. 133**]
4. In the case of legal persons, Member States shall ensure that they may be held liable for infringements referred to in Article 56(1) which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on any of the following:
- (a) a power of representation of the legal person;
 - (b) an authority to take decisions on behalf of the legal person; or
 - (c) an authority to exercise control within the legal person.

^{*} OJ please insert date: *12 months* after the date of entry into force of this Directive.

5. In addition to the cases referred to in paragraph 4 of this Article, Member States shall ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in that paragraph has made possible the commission of the infringements referred to in Article 56(1) for the benefit of a legal person by a person under its authority.

Article 58

1. Member States shall ensure that competent authorities establish effective mechanisms to encourage reporting of breaches of the national provisions implementing this Directive to competent authorities.
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 of institutions who report breaches committed within the institution;
 - (ba) appropriate protection for the accused person; [Am. 134]***
 - (c) protection of personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach, in compliance with the principles laid down in Directive 95/46/EC.

3. Member States shall require obliged entities to have in place appropriate procedures for their employees to report breaches internally through a specific, independent and anonymous channel.

CHAPTER VII FINAL PROVISIONS

Article 59

By ...^{*}, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and to the Council.

By ...^{**}, the Commission shall submit to the European Parliament and to the Council a report on the provisions concerning serious tax offences and punishments in the Member States, on the cross-border significance of tax offences and on the possible need for a coordinated approach in the Union, accompanied if appropriate by a legislative proposal.
[Am. 135]

* OJ please insert date: four years after the date of entry into force of this Directive.

** ***OJ please insert date: one year after the entry into force of this Directive.***

Article 60

Directives 2005/60/EC and 2006/70/EC are repealed with effect from ...*.

References to the repealed directives shall be construed as being made to this Directive and should be read in accordance with the correlation table set out in Annex IV.

Article 61

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by ...*. They shall forthwith communicate to the Commission the text of those measures.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

* OJ please insert date: two years after the entry into force of this Directive.

Article 62

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 63

This Directive is addressed to the Member States.

Done at

For the European Parliament
The President

For the Council
The President

ANNEX I

The following is a non-exhaustive list of risk variables that obliged entities shall consider when determining to what extent to apply customer due diligence measures in accordance with Article 11(3):

- (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 II

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 14:

- (1) Customer risk factors:
 - (a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
 - (b) public administrations or enterprises;
 - (c) customers resident in lower risk geographical areas as set out in point (3);
 - (ca) beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements, and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts; [Am. 136]*
 - (cb) obliged entities where they are subject to requirements to combat money laundering and terrorist financing under this Directive and have effectively implemented those requirements. [Am. 137]*

- (2) Product, service, transaction or delivery channel risk factors:
- (a) life insurance policies where 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 risk of money laundering/terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money as defined in Article 2(2) of Directive 2009/110/EC);
 - (ea) long-term purpose-orientated savings agreements, serving for instance as a safeguard for retirement provisions or for the acquisition of self-used immovable property and where the incoming payments originate from a payment account which is identified in accordance with Articles 11 and 12 of this Directive; [Am. 138]*

- (eb) financial products low in value where repayment is conducted through a bank account in the name of the customer; [Am. 139]*
- (ec) financial products which relate to financial physical assets in the form of leasing agreements or of low value consumer credit, provided the transactions are carried out through bank accounts; [Am. 140]*
- (ed) non-face-to-face business relationships or transactions where the identity is capable of being verified electronically; [Am. 141]*
- (ee) such products, services and transactions identified as low risk by the competent authorities of the home Member State of the obliged entities. [Am. 142]*

(3) Geographical risk factors:

- (a) ~~other~~ Member States; [Am. 143]
- (b) third countries *identified, by credible sources, such as by FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, as* having effective anti-money laundering/combating terrorist financing systems; [Am. 144]
- (c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
- (d) third countries which are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements;
- (da) *jurisdictions identified by the Commission having anti-money laundering measures equivalent to those laid down by this Directive and other related rules and regulations of the Union.* [Am. 145]

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 16(3):

- (1) Customer risk factors:
 - (a) the business relationship is conducted in unusual circumstances;
 - (b) customers resident in countries 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.

- (2) Product, service, transaction or delivery channel risk factors:
 - (a) private banking;
 - (b) products or transactions that *that allow for or that* might favour anonymity; **[Am. 146]**
 - (c) non-face-to-face business relationships or transactions, *without certain safeguards, e.g. electronic signatures*; **[Am. 147]**
 - (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. **[Am. 148]**~~

- (3) Geographical risk factors:
- (a) countries identified by credible sources, such as by FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, as not having effective anti-money laundering/combating terrorist financing 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 *Union or the* United Nations; [**Am. 149**]
 - (d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Annex IIIa

The following are types of enhanced due diligence measures that Member States should as a minimum implement for the application of Article 16:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;*
- Obtaining additional information on the intended nature of the business relationship;*
- Obtaining information on the customer's source of funds or source of wealth of the customer;*
- Obtaining information on the reasons for intended or performed transactions;*
- Obtaining the approval of senior management to commence or continue the business relationship;*
- 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;*
- Requiring the first payment to be carried out through an account opened in the customer's name with a bank subject to similar CDD standards. [Am. 150]*

ANNEX IV

Correlation table referred to in Article 60

Directive 2005/60/EC	This Directive
Article 1	Article 1
Article 2	Article 2
Article 3	Article 3
Article 4	Article 4
Article 5	Article 5
	Articles 6 to 8
Article 6	Article 9
Article 7	Article 10
Article 8	Article 11
Article 9	Article 12
Article 10(1)	Article 10(d)
Article 10(2)	-
Article 11	Articles 13, 14 and 15
Article 12	-
Article 13	Articles 16 to 23
Article 14	Article 24
Article 15	-

Article 16
Article 17
Article 18

Article 19

Article 20
Article 21
Article 22
Article 23
Article 24
Article 25
Article 26
Article 27
Article 28
Article 29
Article 30
Article 31
Article 32

Article 25
-
Article 26
Article 27
Article 28
Article 29
Article 30
-
Article 31
Article 32
Article 33
Article 34
Article 35
Article 36
Article 37
Article 38
-
Article 39
Article 42
Article 40

Article 33	Article 41
Article 34	Article 42
Article 35	Article 43
Article 36	Article 44
Article 37	Article 45
	Article 46
Article 37a	Article 47
Article 38	Article 48
	Articles 49 to 54
Article 39	Articles 55 to 58
Article 40	-
Article 41	-
Article 41a	-
Article 41b	-
Article 42	Article 59
Article 43	-
Article 44	Article 60
Article 45	Article 61
Article 46	Article 62
Article 47	Article 63

Directive 2006/70/EC	This Directive
Article 1	-
Article 2(1), (2) and (3)	Article 3(7)(d), (e) and (f)
Article 2(4)	-
Article 3	-
Article 4	Article 2(2) to (8)
Article 5	-
Article 6	-
Article 7	-