



**COUNCIL OF
THE EUROPEAN UNION**

**Brussels, 12 May 2014
(OR. en)**

9752/14

**Interinstitutional File:
2013/0025 (COD)**

**EF 149
ECOFIN 470
DROIPEN 71
CRIMORG 42
CODEC 1261**

NOTE

From:	Presidency
To:	Delegations
Subject:	Proposal for a DIRECTIVE 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 - 4th Presidency compromise

Delegations will find attached the fourth Presidency compromise on the abovementioned proposal. In the provisions of this Directive, changes are marked by comparison to the revised version of the third Presidency compromise (doc. no. 5786/1/14).

Proposal for a

DIRECTIVE 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 Economic and Social Committee¹,

Having regard to the opinion of the European Central Bank²,

After consulting the European Data Protection Supervisor³,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) Massive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society. In addition to the criminal law approach, a preventive effort via the financial system can produce results.

¹ OJ C , , p. .

² OJ C , , p. .

³ OJ C , , p. .

- (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 certain coordinating measures are not adopted at Union level.
- (3) The current proposal is the fourth Directive to deal with the threat of money laundering. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering⁴ 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 Council of December 2001 amending Council Directive 91/308/EEC⁵ 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 (hereinafter referred to as the 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. These changes were reflected in 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 financing⁶ and 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 basis⁷.
- (4) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even European Union level, without taking account of international coordination and cooperation, would have very limited effects. The measures adopted by the European Union in this field should therefore be consistent with other action undertaken in other international fora. The European Union action should continue to take particular account of the Recommendations of the FATF, which constitutes the foremost international body active in the fight against money laundering and terrorist financing. With the view to reinforce the efficacy of the fight against money laundering and terrorist financing, Directives 2005/60/EC and 2006/70/EC should be aligned with the new FATF Recommendations adopted and expanded in February 2012.

⁴ OJ L 166, 28.6.1991, p. 77.

⁵ OJ L 344, 28.12.2001, p. 76.

⁶ OJ L 309, 25.11.2005, p. 15.

⁷ OJ L 214, 4.8.2006, p. 29.

- (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 crime but also the collection of money or property for terrorist purposes.
- (6) The use of large cash payments is highly vulnerable to money laundering and terrorist financing. In order to increase vigilance and mitigate the risks posed by cash payments natural or legal persons trading in goods should be covered by this Directive to the extent that they make or receive cash payments of EUR 10 000 or more. Member States may decide to adopt stricter provisions including a lower threshold or a general limitation to the usage of cash.
- (6a) The use of electronic money products is increasingly considered as a substitute for bank accounts and therefore, further to Directive 2009/110/EC of the European Parliament and of the Council⁸, warrants subjecting these products to the AML/CFT obligations. However, in certain proven low-risk circumstances and under strict risk mitigating conditions, Member States should be allowed to exempt electronic money products from certain customer due diligence measures, such as the identification and verification of the customer and the beneficial owner. The relevant conditions should include a requirement for exempt electronic money products to be used exclusively for purchasing goods or services and that the amount stored electronically be low enough to preclude circumvention of the AML/CFT rules. This exemption is without prejudice to the discretion given to Member States to allow obliged entities to apply simplified customer due diligence measures to other electronic money products posing lower risks, in accordance with Article 13.
- (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, so as to ensure respect of the rights guaranteed in Articles 7, 47 and 48 of the Charter of Fundamental Rights of the European Union. 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 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 (OJ L 267, 10.10.2009, p. 7.)

- (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 the respect of the rights guaranteed by the Charter of Fundamental Rights of the European Union, 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 expressly highlight that "tax crimes" related to direct and indirect taxes are included in the broad definition of "criminal activity" under this Directive in line with the revised FATF Recommendations. **Since different tax offences may be designated in each Member State as constituting "criminal activity" punishable with the penalties prescribed in Article 3(4)f of this Directive, national law definitions of tax crimes may differ.** While no harmonisation of Member States' national law definitions of tax crimes is sought, ~~such~~ **Member States should ensure that** differences in national definitions **do not should not create any undue restrictions on the provision or exchange of information between EU Financial Intelligence Units (FIUs) and that FIUs strive to provide or exchange all relevant information in this respect.** ~~create any restrictions to the implementation of the provisions of the Directive, especially as regards the reporting obligations and domestic and international cooperation between Financial Intelligence Units (FIUs) and other competent authorities.~~
- (10) There is a need to identify any natural person who exercises ownership or control over a legal entity. In order to ensure effective transparency, Member States should ensure that the widest possible range of legal entities **incorporated or created by any other mechanism in their territory** is covered. While finding a specified percentage shareholding or ownership interest will not automatically result in finding the beneficial owner, it is one evidential factor among others to be taken into account. Identification and verification of beneficial owners should, where relevant, extend to legal entities that own other legal entities and obliged entities should look for the natural person(s) who ultimately exercises control through ownership or control through other means of the legal entity that is the customer. Control through other means may, inter alia, include the criteria of control used for the purposes of preparing consolidated financial statements, such as through shareholders' agreement, the exercise of dominant influence or the power to appoint senior management. There may be cases where no natural person is identifiable who either ultimately owns, or who exerts control over a legal entity. In such exceptional cases obliged entities, having exhausted all other means of identification, and provided there are no grounds **for suspicion** ~~to suspect that such a natural person exists,~~ **may** ~~should~~ consider the senior managing official(s) as beneficial owner(s).

- (11) The need for accurate and up-to-date information on the beneficial owner is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. Member States should therefore ensure that corporate and other legal entities, ~~including foundations,~~ obtain and hold adequate, accurate and current information on their beneficial ownership and that this information **is provided to obliged entities when the latter are taking customer due diligence measures and** is made available to competent authorities, ~~and~~ FIUs ~~and is provided to obliged entities.~~ With a view to enhancing transparency, **beneficial ownership information should be stored in** specified locations, ~~such as~~ **for example in the case of companies in a public central company registry in the case of companies** registries of legal entities, [...] or ~~other suitable mechanisms, including data retrieval systems,~~ satisfying strict criteria **of timely and unrestricted access to the information stored.** ~~should be used for storing information on beneficial ownership.~~ In order to ensure a level playing field among different types of legal form, trustees should also be ~~obliged~~ **required to obtain, hold and provide to obliged entities taking customer due diligence measures, beneficial ownership information and to** communicate **this** ~~beneficial ownership information to the specified locations or data retrieval systems~~ ~~other suitable mechanisms~~ and they should declare their status to obliged entities.
- (12) This Directive should also apply to those activities of the obliged entities covered by this Directive which are performed on the internet.
- (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, an obligation for providers of gambling services posing higher risks to conduct customer due diligence for single transactions of EUR 2 000 or more should be laid down. Member States should **consider applying** this threshold to the collection of winnings and/or wagering a stake, including by the purchase and exchange of gambling chips. 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. However in proven low-risk circumstances, Member States should be allowed to exempt certain gambling services from some or all of the Directive's requirements. The use of an exemption by a Member State should only be considered in strictly limited and justified circumstances, and where the money laundering or terrorist financing risks are negligible. Such exemptions should be subject to a specific risk assessment and be notified to the Commission.
- (14) The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a risk-based approach 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 European Union and those operating within it.

- (15) Underpinning the risk-based approach is a need for Member States 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) (hereinafter ‘EBA’), established by 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)⁹; the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (hereinafter ‘EIOPA’), established by 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)¹⁰; and the European Supervisory Authority (European Securities and Markets Authority) (hereinafter ‘ESMA’), established by 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)¹¹, should be tasked with issuing an opinion on the risks affecting the EU financial sector.
- (15a) The Commission is well placed to review specific cross-border threats, that could affect the internal market and which cannot be identified and effectively combatted by individual Member States. Therefore, it should be entrusted with the responsibility of coordinating the assessment of the above-mentioned risks related to cross-border phenomena and with making recommendations on the appropriate measures to tackle the identified risks. Involvement of the relevant experts, such as the Expert Group on Money Laundering and Terrorist Financing and the representatives from the Member States' FIUs, as well as - where appropriate - other EU level bodies, is essential for the effectiveness of this process.
National risk assessments and experiences are also an important source of information for the process.
- (16) The results of risk assessments at Member State level should, where appropriate, be made available to obliged entities to enable them to identify, understand and mitigate their own risks.
- (17) In addition, to even better understand and mitigate risks at European Union level, Member States should share the results of their risk assessments with each other, the Commission and EBA, EIOPA and ESMA.

⁹ OJ L 331, 15.12.2010, p. 12.

¹⁰ OJ L 331, 15.12.2010, p. 48.

¹¹ OJ L 331, 15.12.2010, p. 84.

- (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.
- (18a) In order to ensure uniform conditions for the protection of the proper functioning of the EU financial system and of the Internal Market from money laundering and terrorist financing, it is important that the Commission identifies third country jurisdictions which have strategic deficiencies in their national AML/CFT regimes (hereinafter referred to as ‘high-risk third countries’). The changing nature of money laundering and terrorist financing threats, facilitated by a constant evolution of technology and of the means at the disposal of criminals, requires that quick and continuous adaptations of the legal framework as regards high-risk third countries be made in order to efficiently address existing risks and prevent new ones from arising. The Commission should take into account information from international organisations and standard setters in the field of anti-money laundering and ~~countering terrorist~~ **the financing of terrorism (AML/CFT)**, such as FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, and adapt its assessments to the changes therein, where appropriate.
- (18b) Member States should at least provide for enhanced customer due diligence measures to be applied by the obliged entities when dealing with persons or legal entities established in high-risk third countries identified by the Commission. Equally, reliance on third parties established in such high-risk third countries should be prohibited. **Countries not included in the list should not automatically be considered as having effective AML/CFT systems and their entities should be assessed on a risk sensitive basis.**
- (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 holding, or having held, important public positions, particularly those from countries where corruption is widespread. 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.
- (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.
- (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 only arise from contract and not from this Directive. The responsibility for complying with this Directive should remain with the obliged entity covered hereby.
- (25) All Member States have, or should, set up operationally independent and autonomous financial intelligence units (hereinafter referred to as 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 and other information relevant to money laundering, associated predicate offences and terrorist financing should be reported to the FIUs, which should serve as a national centre for receiving, analysing and disseminating to the competent authorities the results of its analysis. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction. Reported information may also include threshold based information.

- (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.
- (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 employees who report their suspicions of money laundering being subjected 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~~ AML/CFT system. Member States should be aware of this problem and should do whatever they can to protect employees or persons in a comparable position from such threats or hostile action.
- (30) 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 data¹², as implemented in national law, is applicable to the processing of personal data for the purposes of this Directive.

¹² OJ L 281, 23.11.1995, p. 31.

- (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 of 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, sharing of information by competent authorities and sharing of information by credit and financial institutions. 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.
- (32) The fight against money-laundering and terrorist financing is recognised as an important public interest ground by all Member States.
- (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.
- (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 to this right in accordance with the rules laid down in Article 13 of Directive 95/46/EC are therefore justified.
- (35) Persons who merely convert paper documents into electronic data and are acting 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 and financial institutions have branches and subsidiaries located in third countries where the legislation in this 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, 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 EU-wide situation with respect to the fight against money laundering and terrorist financing and publish regular overviews.
- (37a) Where Member States decide to require issuers of electronic money and payment service providers established on their territory in forms other than a branch, and whose head office is situated in another Member State, to appoint a central contact point in their territory, they **may require** ~~should ensure that such a~~ **central contact point, acting on behalf of the appointing institution, ensures the establishments' compliance with AML/CFT rules. They should also ensure that this** requirement is proportionate and does not go beyond what is necessary to achieve the aim of ~~overseeing~~ **ensuring** the compliance with ~~anti-money laundering and terrorist financing~~ **AML/CFT rules, including by facilitating the respective supervision.**
- (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.
- (38a) Where an obliged entity operates establishments in another Member State, including through a network of agents, the home country's competent authority is responsible for supervising the obliged entity's application of group AML/CTF policies and processes. This may involve on-site visits in establishments based in another Member State. The home country's competent authority should cooperate closely with the host country's competent authority and inform the host country's competent authority of any issues that could affect their assessment of the establishment's compliance with the host country's AML/CFT obligations.

- (38b) Where an obliged entity operates establishments in another Member State, including through a network of agents **or persons distributing electronic money according to Article 3 (4) of Directive 2009/110/EC**, the host country's competent authority retains responsibility for enforcing the establishment's compliance with ~~the~~ AML/CTF requirements, including, **where appropriate**, by carrying out onsite inspections and offsite monitoring **and by taking appropriate and proportional measures to remove serious infringements of these requirements**. The host country's competent authority should cooperate closely with the home country's competent authority and inform the home country's competent authority of any issues that could affect their assessment of the obliged entity's application of group AML/CTF policies and processes. **In order to remove serious infringements of AML/CFT rules that require immediate remedies, the host country's competent authority may be empowered to apply appropriate and proportionate temporary remedial measures, applicable under similar circumstances to obliged entities under their competence, to address such serious failings, where appropriate, with the assistance of, or in cooperation with the home country's competent authority.**
- (39) Taking into account the transnational character of money laundering and terrorist financing, co-ordination and co-operation between EU FIUs are extremely important. ~~This co-operation has so far only been addressed by 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 information¹³.~~ In order **to improve such** ~~to ensure better co-ordination and administrative 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 enhanced up-dated rules should be included in this Directive.~~
- (39a) The "EU Financial Intelligence Units' Platform", an informal group composed of representatives from Member States' FIUs and active since 2006, is used to facilitate cooperation among national FIUs and exchange views on co-operation related issues such as effective international FIUs co-operation, the joint analysis of cross-border cases as well as trends and factors relevant to assessing money laundering and terrorist financing risks both on the national and supranational level.

¹³ — OJ L 271, 24.10.2000, p. 4.

- (40) Improving the exchange of information between FIUs within the EU 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 FIU.net network or its successor and the techniques offered by that network, should be encouraged by Member States. The initial exchange between the FIUs of information related to money laundering or terrorist financing for analytical purposes and which is not further processed or disseminated should be allowed unless it would compromise the legitimate interests of the Member State or of a natural or legal person. **Exchanges of information on cases identified by EU FIUs as possibly involving tax crimes should be without prejudice to exchanges of information in the field of taxation, in accordance with Council Directive 2011/16/EU on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC¹⁴ or in accordance with international standards on the exchange of information and administrative cooperation in tax matters.**
- (40a) In order to be able to respond fully and rapidly to enquiries from FIUs, obliged entities need to have in place effective systems enabling them to have full and timely access through secure and confidential channels to information about business relationships that they maintain or have maintained with specified legal or natural persons. Member States could, for instance, consider putting in place systems of banking registries or electronic data retrieval systems which would provide FIUs with access to information on bank accounts. Member States could also consider establishing mechanisms to ensure that competent authorities have procedures in place in order to identify assets without prior notification to the owner.
- (40b) Member States should encourage their competent authorities to rapidly, constructively and effectively provide the widest range of international cooperation for the purposes of this Directive, including the exchange of information between non-counterpart authorities amongst Member States.

- (41) The importance of combating money laundering and terrorist financing should lead Member States to lay down effective, proportionate and dissuasive administrative measures and penalties 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 penalties for breaches of the key preventative provisions. This diversity could be detrimental to the efforts made in 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 penalties that Member States shall **at least** have available for serious, repetitive or systematic breaches of the requirements relating to customer due diligence measures, record keeping, reporting of suspicious transactions and internal controls of obliged entities. This range should be sufficiently broad to allow Member States and competent authorities to take account of the differences between obliged entities, in particular between credit and financial institutions and other obliged entities, as regards their size, characteristics and areas of activity. In the application of this Directive, Member States should ensure that the imposition of administrative measures and penalties in accordance with this Directive and of criminal penalties in accordance with national law does not breach the principle of *ne bis in idem*.
- (41a) For the purposes of assessing the appropriateness of persons holding a management function in or otherwise controlling obliged entities, an efficient system of exchange of information is required where EBA, EIOPA and ESMA subject to data protection requirements, should be entitled to maintain a central database containing details of administrative penalties and measures applied to credit and financial institutions, including any appeals in relation thereto, which is accessible to competent authorities only. **In any event, information about criminal convictions should be exchanged in accordance with Framework Decision 2009/315/JHA¹⁵ and Decision 2009/316/JHA¹⁶, as transposed into national law, and with other relevant provisions of national law.** ~~This exchange of information shall be without prejudice to information about criminal convictions exchanged by Member States in accordance with the relevant provisions of their national law, and in particular those transposing into their national law Framework Decision 2009/315/JHA and Decision 2009/316/JHA.~~
- (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 EBA, EIOPA and ESMA with the elaboration of draft regulatory technical standards which do not involve policy choices, for submission to the Commission.

15

16

- (43) The Commission should adopt the draft regulatory technical standards developed by EBA, EIOPA and ESMA pursuant to Article 42 of this Directive by means of delegated acts pursuant to Article 290 of the Treaty on the Functioning of the European Union and in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010, Regulation (EU) No 1094/2010 and Regulation (EU) No 1095/2010.
- (44) In view of the very substantial amendments that would need to be made to Directive 2005/60/EC and Directive 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 and can therefore, 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 of Fundamental Rights of the European Union, in particular, the respect for private and family life, 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.
- (47) In line with Article 21 of the EU Charter of Fundamental Rights 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,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

SECTION 1

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 assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
 - (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/JHA of 13 June 2002 on combating terrorism¹⁷, as amended by Council Framework Decision 2008/919/JHA of 28 November 2008¹⁸.
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.

Article 2

1. This Directive shall apply to the following obliged entities:
 - (1) credit institutions;
 - (2) financial institutions;
 - (3) the following legal or natural 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 real estate 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;

¹⁷ OJ L 164, 22.6.2002, p. 3.

¹⁸ OJ L 330, 9.12.2008, p. 21-23.

- (iv) organisation of contributions necessary for the creation, operation or management of companies;
- (v) creation, operation or management of trusts, companies or similar structures;
- (c) trust or company service providers not already covered under points (a) or (b);
- (d) real estate agents;
- (e) other natural or legal persons trading in goods, only to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;
- (f) providers of gambling services.

1a. With the exception of casinos and online gambling and following an appropriate risk assessment, Member States may decide to exempt fully or in part providers of certain gambling services from national provisions transposing the provisions of this Directive on the basis of the proven low risk posed by the nature and, **where appropriate, the** scale of operations of such services ~~providers~~.

Any decision taken by a Member State pursuant to this paragraph shall be notified, along with a justification based on a specific risk assessment, to the Commission, ~~who shall verify that exemptions are used in strictly limited and justified circumstances.~~ **The Commission shall communicate the decision to the other Member States.**

~~If, after receiving all necessary information pursuant to the previous subparagraph, the Commission considers that an exemption is not justified by proven low risk, it shall, within three months, ask the Member State to refrain from granting the exemption. In the absence of a response from the Commission within the abovementioned deadline, the exemption may be granted.~~

2. Member States may decide that legal and natural persons, who 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 legal or natural 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 mentioned 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 previous subparagraph shall not apply to the legal and natural 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 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/EC¹⁹.

3. For the purposes of point (a) of paragraph 2, Member States shall require that the total turnover of the financial activity may 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.
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 legal or natural person concerned.

¹⁹ OJ L 319, 5.12.2007, p. 1.

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 taken by a Member State pursuant to paragraph 2 shall state the reasons on which it is based. Member States shall provide for the possibility of withdrawing that decision should circumstances change. Such a decision shall be made available **to the Commission. The Commission shall communicate the decision**, ~~on request,~~ to **the** other Member States.
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 Article 3(1) of 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, including branches within the meaning of Article 3(16) of that Directive located in the European Union of credit institutions having their head offices inside or outside the European Union;
- (2) "financial institution" means:
 - (a) an undertaking, other than a credit institution, which carries out one or more of the operations included in points 2 to 12 and points 14 and 15 of Annex I to Directive 2013/36/EU, including the activities of currency exchange offices (bureaux de change);

- (b) an insurance company **as defined** ~~duly authorised in Article 13 point (1) of accordance with Directive 2009/138/EC 2002/83/EC~~ of the European Parliament and of the Council of ~~5-25~~ November ~~2002-2009~~ **on the taking up and pursuit of the business of Insurance and Reinsurance (Solvency II)** ²⁰ ~~(1)~~ concerning life assurance ²¹, insofar as it carries out activities covered by that Directive ~~and other investment related services~~;
- (c) an investment firm as defined in point 1 of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments²²;
- (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 Council of 9 December 2002 on insurance mediation²³ when they act in respect of life insurance and other investment related services, with the exception of intermediaries as mentioned in Article 2(7) of that Directive;
- (f) branches, when located in the European Union, of financial institutions as referred to in points (a) to (e), whose head offices are inside or outside the European Union;
- (3) "property" means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;
- (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 on combatting terrorism, as amended by Council Framework Decision 2008/919/JHA of 28 November 2008;
- (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;

²⁰ **OJ L 335, 17.12.2009, p. 1.**

~~²¹ OJ L 345, 19.12.2002, p. 1.~~

²² OJ L 145, 30.4.2004, p. 1.

²³ OJ L 9, 15.1.2003, p. 3.

- (c) the activities of criminal organisations as defined in Article 1 of 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 Union²⁴;
- (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 Interests²⁵;
- (e) corruption;
- (f) all offences, including tax crimes, as defined in national law of the Member States, 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.

~~Differences between national law definitions of tax crimes should not impede the ability of FIUs and other competent authorities to cooperate and exchange information both domestically and across borders within the EU, especially as regards information on suspicions of money laundering and terrorist financing;~~

- (5) "beneficial owner" means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:
 - (a) in the case of corporate entities:
 - (i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership over a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer share holdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union legislation or subject to equivalent international standards which ensure adequate transparency of ownership information.

²⁴ OJ L 351, 29.12.1998, p. 1.

²⁵ OJ C 316, 27.11.1995, p. 49.

A shareholding or ownership interest of [...] 25% or more in the customer held by a natural person shall be an indication of direct ownership.

A shareholding or ownership interest of [...] 25% or more in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership.

~~The notion of e~~Control **through other means may** shall be determined, inter alia, in accordance with the criteria in Article 22(1) to (5) of 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 undertakings²⁶.

- (ii) if, after having exhausted all possible means **and provided there are no grounds for suspicion**, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s);

- (b) in the case of trusts ~~or similar legal arrangements or legal entities, such as foundations, [...] which administer and distribute funds:~~
 - (i) the settlor;
 - (ii) the trustee(s);
 - (iii) the protector, if any;
 - (iv) the beneficiaries; or 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;
 - (v) any other natural person exercising ultimate control over the trust ~~or other~~ through direct or indirect ownership or through other means.

- (c)** In the case of legal arrangements ~~other than trusts or~~ **and** legal entities **similar to trusts, such as foundations**, the natural person(s) holding equivalent or similar positions to those under points **(b) (i) to (iii)** shall be included;

²⁶ OJ L 182, 29.6.2013, p.19.

- (6) "trust or company service providers" 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 European Union legislation or subject to equivalent international standards;
- (6a) "correspondent relationship" means:
- (a) the provision of banking services by one bank (the "correspondent") to another bank (the "respondent"), including but not limited to providing a current or other liability account and related services, like cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;
 - (b) the relationships between credit institutions, financial institutions and among credit and financial institutions where similar services are provided, including but not limited to those relationships established for securities transactions or funds transfers;
- (7) (a) "politically exposed persons" means natural persons who are or have been entrusted with prominent public functions and includes the following:
- (b) *deleted*
 - (c) *deleted*

- (d) *deleted*
- (i) heads of State, heads of government, ministers and deputy or assistant ministers;
 - (ii) members of parliaments;
 - (ia) members of the governing bodies of political parties;
 - (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) members of the administrative, management or supervisory bodies of State owned enterprises;
 - (vii) directors, deputy directors and members of the board or equivalent function of an international organisation.

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

(7a) "family members" **includes** ~~means~~ the following:

- (i) the spouse;
- (ii) any person considered as equivalent to the spouse;
- (iii) the children and their spouses or persons considered as equivalent to the spouse;
- (iv) the parents;

(7b) "persons known to be close associates" means the following:

- (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 point (7);

- (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 a person referred to in point (7);
- (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;
- (11) "group" means a group of undertakings, which consists of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU.

Article 4

1. Member States shall 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.
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.

SECTION 2

RISK ASSESSMENT

Article 6

- 1. The Commission shall coordinate work at the EU level on the identification, understanding and assessment of money laundering and terrorist financing risks affecting the internal market and related to specific cross-border phenomena and shall draw up a report on these risks. The Commission shall take into account the joint opinion by EBA, EIOPA and ESMA, referred to in paragraph 2 of this Article, when available, and involve the Member States' experts in the area of anti-money laundering and countering ~~terrorist~~ the financing of terrorism (AML/CFT), representatives from Member States' FIUs and other EU level bodies where appropriate.

The first report shall be provided by ... [two years from the date of entry into force of this Directive] and subsequent reports shall be provided as necessary. The reports shall be published.

1. The European Banking Authority (hereinafter "EBA"), European Insurance and Occupational Pensions Authority (hereinafter "EIOPA") and European Securities and Markets Authority (hereinafter "ESMA") shall provide a joint opinion on the money laundering and terrorist financing risks affecting the EU financial sector.

The first opinion shall be provided by ... [18 months from the date of entry into force of this Directive] and subsequent opinions shall be provided as necessary.

2. The Commission shall make the opinions referred to in paragraph 1 available to assist Member States and obliged entities to identify, manage and mitigate the risk of money laundering and terrorist financing.

3. *deleted*

4. *deleted*

5. The Commission shall make recommendations to Member States on the measures suitable for addressing the identified risks. In case Member States decide not to apply any of the recommendations in their national AML/CFT regimes they shall notify the Commission thereof and provide a justification for such a decision.

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, and keep the assessment up-to-date.
2. Each Member State shall designate an authority or establish a mechanism to co-ordinate the national response to the risks referred to in paragraph 1. The identity of that authority or the description of the mechanism shall be notified to the Commission, EBA, EIOPA and ESMA and other Member States.
3. In carrying out the assessments referred to in paragraph 1, Member States may make use of the opinion referred to in Article 6(1) and the findings of the report 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~~ **AML/CFT** regime, in particular by identifying any areas where obliged entities shall apply enhanced measures and, where appropriate, specifying the measures to be taken;
 - (b) use the assessment(s) to assist it in the allocation and prioritisation of resources to combat money laundering and terrorist financing;
 - (c) make appropriate information available to obliged entities to carry 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 EBA, EIOPA and ESMA.

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. These 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 to the relevant competent authorities and self-regulatory bodies concerned. Competent authorities may decide that individual documented risk assessments are not required, if the specific risks inherent in the sector are clear and understood.
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.
4. The policies and procedures referred to in paragraph 3 shall at least include:
 - (a) the development of internal policies, procedures and controls, including 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;
 - (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.

SECTION 3

THIRD COUNTRY POLICY

Article 8a

- 1. **Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the European Union, shall be identified in order to protect the proper functioning of the Internal Market.**

1. The Commission shall be empowered to adopt implementing acts to identify high-risk third countries ~~that pose significant threats to the financial system of the European Union~~ **referred to in paragraph 1**, taking into account strategic deficiencies, in particular in relation to:
 - (a) the legal and institutional ~~anti-money laundering and counter terrorist financing~~ **AML/CFT** framework of the third country, in particular:
 - (i) the criminalization of money laundering and terrorist financing,
 - (ii) customer due diligence measures,
 - (iii) record keeping requirements, and
 - (iv) suspicious transaction reporting;
 - (b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing; or
 - (c) the effectiveness of the anti-money laundering and counter terrorist financing system in addressing money laundering or terrorist financing risks of the third country.
2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in **paragraph 2 of** Article 58c~~(2)~~.
3. The Commission shall take into account, where appropriate, relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competencies in the field of **preventing** ~~anti-money laundering and the prevention of~~ **combating** ~~terrorist~~ **the financing of terrorism** in relation to the risks posed by individual third countries.

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. Member States shall in all cases require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks 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.

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 an occasional transaction:
 - (i) 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; or
 - (ii) which constitutes a transfer of funds according to Article 2, paragraph 7 of [revised Reg 1781/2006] exceeding EUR 1 000;
- (c) for natural or legal persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

- (d) for providers of gambling services, either upon the collection of winnings and/or upon the wagering of a stake, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- (e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- (f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 10 bis

1. By way of derogation from Articles 11 and 12 and based on an appropriate risk assessment which demonstrates low risk, Member States may decide to allow obliged entities not to apply certain customer due diligence measures in respect of electronic money, as defined in Article 2(2) of Directive 2009/110/EC, if all of the following risk mitigating conditions are fulfilled:
 - (a) the payment instrument is not reloadable **or it is a SIM card with a maximum monthly payment transactions limit EUR 250.**
 - (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 anonymous electronic money;
 - (e) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.
2. Member States shall ensure that the derogation set out in paragraph 1 is not applicable in case of redemption in cash **or cash withdrawal** of the monetary value of the electronic money where the amount redeemed exceeds EUR ~~250~~**100**.

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 the beneficial owner and taking reasonable measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
 - (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.

Obligated entities shall also be required when performing the measures in points (a) and (b) above, to verify that any person purporting to act on behalf of the customer is so authorised and shall be required to identify and verify the identity of that person.

2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements set out in paragraph 1, but obliged entities may determine the extent of such measures on a risk-sensitive basis.
3. Member States shall require that obliged entities take into account at least the variables set out in Annex I when assessing money laundering and terrorist financing risks.
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 credit and 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 credit or 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), the verification of the identity of the beneficiaries shall occur at the time of the payout. In case of assignment, in whole or in part, of the life or other investment related insurance to a third party, credit and financial institutions aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for own benefit the value of the policy assigned.

6. For beneficiaries of trusts that are designated by characteristics or by class, obliged entities shall obtain sufficient information concerning the beneficiary to satisfy themselves that they 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.

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 if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

3. By way of derogation from paragraph 1, Member States may allow the opening of an account with a credit or financial institution, including accounts that permit transactions in transferable securities, 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 obligations set out in Article 11(1)(a) and (b) 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 terminate the business relationship and consider making a suspicious transaction report to the FIU in accordance with Article 32 in relation to the customer.

Member States shall not apply the first subparagraph to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such 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 and is necessary to ensure respect of the rights guaranteed in the Articles 7, 47 and 48 of the Charter of Fundamental Rights of the European Union.

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 or business relationship to enable the detection of unusual or suspicious transactions.

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 potentially lower risk situations set out in Annex II.

Article 15

EBA, EIOPA and ESMA shall 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 shall be taken of the nature and size of the business, and where appropriate and proportionate, specific measures foreseen. These guidelines shall be issued within 2 years of 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 when dealing with natural persons or legal entities established in the third countries, identified by the Commission as high-risk in accordance with Article 8a, also in other cases of higher risks 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.

Enhanced customer due diligence measures need not be invoked automatically with respect to branches and majority-owned subsidiaries of obliged entities established in the European Union which are located in the third countries, identified by the Commission as high-risk in accordance with Article 8a, if these branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 42. Member States shall ensure that these cases are handled by obliged entities by using a risk-based approach.

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. 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 suspicious.
3. When assessing the money laundering and terrorist financing risks, Member States and obliged entities shall take into account at least the factors of potentially higher-risk situations set out in Annex III.
4. EBA, EIOPA and ESMA shall 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 enhanced due diligence measures are appropriate. Specific account shall be taken of the nature and size of the business, and where appropriate and proportionate, specific measures foreseen. Those guidelines shall be issued within 2 years of the date of entry into force of this Directive.

Article 17

In respect of cross-frontier correspondent 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 and financial 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~~ AML/CFT controls;
- (c) obtain approval from senior management before establishing new correspondent relationships;
- (d) document the respective responsibilities of each institution;
- (e) with respect to payable-through accounts, be satisfied that the respondent credit or financial 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 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 management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is such a person;
- (b) in cases of business relationships with such persons, apply the following measures:
 - (i) *deleted*
 - (ii) obtain senior management approval for establishing or continuing business relationships with such customers;
 - (iii) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;
 - (iv) conduct enhanced ongoing monitoring of the business relationship.

Article 19

deleted

Article 20

Obligated entities shall take reasonable measures to determine whether the beneficiaries of a life or other investment related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. 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 obliged entities to:

- (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 and 20 shall also apply to family members or persons known to be close associates of such politically exposed persons.

Article 22

Where a person referred to in Articles 18 and 20 has ceased to be entrusted with a prominent public function by a Member State or a third country or 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. This period of time shall not be less than 18 months.

Article 23

1. Member States shall prohibit credit and financial institutions from entering into or continuing a correspondent relationship with a shell bank and shall require that those institutions take appropriate measures to ensure that they do not engage in or continue correspondent relationships with a credit or financial institution 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 or financial 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.

Article 25

1. For the purposes of this Section, "third parties" shall mean obliged entities who are listed in Article 2, or other institutions and persons situated in Member States or a third country, who apply customer due diligence requirements and record keeping requirements consistent with those laid down in this Directive, and whose compliance with the requirements of this Directive is supervised consistent with Section 2 of Chapter VI.
2. Member States shall prohibit obliged entities from relying on third parties established in third countries indicated by the Commission as high-risk in accordance with Article 8a. Member States may exempt branches and majority-owned subsidiaries of obliged entities established in the European Union from the abovementioned prohibition if these branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 42.

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

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 complies with the measures contained in Article 25 and 26 through its group programme, where the following conditions are fulfilled:

- (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 competent authority.

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.

CHAPTER III

BENEFICIAL OWNERSHIP INFORMATION

Article 29

1. Member States shall ensure that corporate and other legal entities incorporated ~~or formed~~ within their territory obtain and hold adequate, accurate and current information on their beneficial ownership. Member States shall ensure that these entities **are required to provide essential information and documentation, including information concerning the beneficial owner,** ~~provide, in a timely manner, this information~~ to obliged entities, when the obliged entities are taking customer due diligence measures in accordance with Article 10.
2. Member States shall ensure that the information referred to in paragraph 1 is held in a specified location, **for example in the case of companies in a public and central company registry,** ~~or by means of other suitable mechanisms,~~ **or in data retrieval systems,** which ensure timely and unrestricted access by competent authorities, ~~including~~ **and** FIUs, without alerting the entity concerned.

Member States shall notify to the Commission the characteristics of the national mechanism used to hold beneficial ownership information.
3. *deleted*
4. Member States may allow obliged entities to access information on beneficial ownership referred to in paragraph 2 and lay down the conditions to this effect.
5. Member States shall ensure that competent authorities and FIUs are able to provide information referred to in paragraphs 1 and 2 to the competent authorities and FIUs of other Member States in a timely manner.
6. This Article does not exempt obliged entities from their customer due diligence obligations laid down in this Directive. Those obligations shall be fulfilled by using a risk-based approach.

7. Member States shall provide for adequate and proportionate sanctions where **corporate and other** legal entities repetitively or systematically fail to comply with the requirements to obtain and disclose information on their beneficial owners in accordance with this Article.
8. Member States shall take measures to prevent misuse of bearer shares and bearer share warrants.

Article 30

1. Member States shall **require** ~~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, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and of any other natural person exercising effective control over the trust.

- ~~1a. Member States shall ensure that the trustees of express trusts governed under their law, provide, in a timely manner, the information referred to in paragraph 1 to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Article 10.~~
2. Member States shall ensure that trustees disclose their status **and provide in a timely manner the information referred to in paragraph 1** to obliged entities, **when the obliged entities are taking customer due diligence measures in accordance with Article 10 and, in particular,** 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~~ **require** that the information referred to in paragraphs 1 ~~and 1a~~ is held in a specified location or **in data retrieval systems** ~~by means of other suitable mechanisms~~ which ensure timely and unrestricted access by competent authorities and FIUs without alerting the parties to the trust concerned.
4. Member States shall ensure that competent authorities and FIUs are able to provide information referred to in paragraph 1 to the competent authorities and FIUs of other Member States in a timely manner.
5. *deleted*

6. This Article does not exempt obliged entities from their customer due diligence obligations laid down in this Directive. Those obligations shall be fulfilled by using a risk-based approach.
7. Member States shall provide for adequate and proportionate sanctions where trustees repetitively or systematically fail to comply with the requirements referred to in this Article.
8. Member States shall ensure that the measures provided for in this Article apply to other types of legal entities and arrangements with a structure or functions similar to trusts.

CHAPTER IV

REPORTING OBLIGATIONS

SECTION 1

GENERAL PROVISIONS

Article 31

1. Each Member State shall establish an FIU in order to effectively combat money laundering and terrorist financing.
2. Member States shall notify the Commission in writing of the name and address of the respective FIUs.
3. The FIU shall be operationally independent and [...] autonomous. The FIU as the central national unit **shall be** responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. The FIU shall be responsible for disseminating ~~such information and~~ the results of its analysis **and any additional relevant information** to the competent authorities when there are grounds to suspect money laundering, associated predicate offences or terrorist financing. It shall be able to obtain additional information from obliged entities.

The FIU shall be provided with adequate financial, human and technical resources in order to fulfil its tasks.

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. FIUs shall be able to respond to requests for information by competent authorities in their Member State when these are motivated by money laundering associated predicate offences and terrorist financing concerns. The decision on conducting the analysis or dissemination of information shall remain with the FIU. Where 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 divulgation of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested the FIU is under no obligation to comply with the request. Member States shall require competent authorities to provide feedback to the FIU about the use made of the information provided in accordance with this Article and about the outcome of the investigations or inspections performed on its basis.
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, confirm the suspicion and disseminate the results of the analysis to competent authorities. The FIU shall be empowered to take such action at the request of an FIU from another Member State for the periods and under the conditions specified in the national law of the FIU receiving the request.
6. The FIU's analysis function shall consist of the following:
 - (a) an operational analysis which focusses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use after dissemination; and
 - (b) 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:
 - (a) by promptly informing, including by filing a report, the FIU, on their own initiative, where the obliged entity 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) by promptly furnishing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable legislation.

All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

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 obliged entity forwarding the information is established. The person or persons designated in accordance with the procedures provided for in Article 8(4) shall forward the information.

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) designate an appropriate self-regulatory body of the profession concerned as the authority to receive the information referred to in Article 32(1).

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 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, and ensures respect of the rights guaranteed in Articles 7, 47 and 48 of the Charter of Fundamental Rights of the European Union.

Article 34

1. Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to funds that are proceeds of criminal activity or are related to terrorist financing, until they have completed the necessary action in accordance with Article 32(1)(a) and complied with any further specific instructions from the competent authorities in conformity with the legislation of the relevant Member State.
2. Where such a transaction is suspected to involve funds that are related to money laundering, associated predicate offences or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected 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

The disclosure in good faith as foreseen in Articles 32 (1) and 33 by an obliged entity or by an employee or director of such an obliged entity of the information referred to in 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 even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Article 37

Member States shall take appropriate measures in order to protect directors, employees, or persons in a comparable position, of the obliged entity who report suspicions of money laundering or terrorist financing either internally or to the FIU from being exposed to threats or hostile action.

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 is being, will be or has been transmitted in accordance with Articles 32 and 33 or that a money laundering or terrorist financing analysis 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, or disclosure for law enforcement purposes.
3. The prohibition laid down in paragraph 1 shall not prevent disclosure between obliged entities from Member States referred to in Article 2(1)(1) and (2), or entities 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 obliged entities 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 or compliance control.

5. For obliged entities 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 obliged entities, 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.
6. Where the obliged entities referred to in Article 2(1)(3)(a) and (b) seek to dissuade a client from engaging in illegal activity, this shall not constitute a disclosure within the meaning of paragraph 1.

CHAPTER V

RECORD KEEPING AND STATISTICAL DATA

Article 39

Member States shall require obliged entities to retain 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 of the documents, evidence and information obtained, for a period of five years after the occasional transaction was carried out or after the business relationship with their customer has ended. Upon expiration of that five-year 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. **In such a case t**~~The~~ maximum retention period shall not exceed ~~th~~ **the limitation period provided for in their national law and, in any case, fifteen** ~~ten~~-years;
- (b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of five years following either the carrying-out of the transactions or the end of the business relationship, whichever period expires first. Upon expiration of this 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. **In such a case t**~~The~~ maximum retention period following either the carrying-out of the transactions or the end of the business relationship, whichever period expires first, shall not exceed **the limitation period provided for in their national law and, in any case, fifteen** ~~ten~~-years.

Article 40

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.

Article 41

1. Member States shall, for the purposes of contributing to 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~~AML/CFT regime, including the number of suspicious transaction reports made to the FIU, the follow-up given to these reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences, the types of predicate offences, where such information is available, and the value in euro of property that has been frozen, seized or confiscated.
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, in addition to the obligations under this Directive binding individual obliged entities, 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 AML/CFT ~~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.

- 1a. Member States shall require that obliged entities that operate establishments in another Member State ensure that these establishments respect the national provisions of that other Member State pertaining to this Directive.
2. Member States shall ensure that where obliged entities have branches or majority-owned subsidiaries located in third countries where the minimum ~~AML/CFT 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, EBA, EIOPA and ESMA shall inform each other of cases where the legislation of the third country 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 the legislation of the third country does not permit application of the measures required under paragraph 1, obliged entities ensure that branches and majority owned subsidiaries in this third country apply 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 exercise additional supervisory actions, including, requiring that the group does not establish or ~~that it terminates~~ business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the third country concerned.
5. EBA, EIOPA and ESMA 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 in Article 2(1)(1) and (2) where the legislation of the third country does not permit application of the measures required under paragraphs 1 and 2. EBA, EIOPA and ESMA shall submit those draft regulatory technical standards to the Commission within two years of the date of entry into force of this Directive.
6. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 5 in accordance with the procedure laid down in 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. Information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group, unless otherwise instructed by the FIU.

8. Member States may require issuers of electronic money as defined by Directive 2009/110/EC of the European Parliament and of the Council²⁷ and payment service providers as defined by Directive 2007/64/EC of the European Parliament and of the Council²⁸ established on their territory in forms other than a branch, and whose head office is situated in another Member State, to appoint a central contact point in their territory to **ensure on behalf of the appointing institution** ~~oversee the compliance with **AML/CFT** anti-money laundering and terrorist financing rules and **to facilitate supervision by competent authorities, including by**~~ **provide** ~~providing~~ competent authorities with documents and information on request.
9. EBA, EIOPA and ESMA shall develop draft regulatory technical standards ~~on the~~ **setting out exhaustive** criteria for determining the circumstances when the appointment of a central contact point pursuant to paragraph 8 above is appropriate, and what the functions of central contact points should be. EBA, ESMA and EIOPA shall submit these draft regulatory technical standards to the Commission within two years of the date of entry into force of this Directive.
10. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 9 in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010.

Article 43

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

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

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

²⁷ OJ L 267, 10.10.2009, p. 7.

²⁸ OJ L 319, 5.12.2007, p. 1.

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, wherever practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided.

SECTION 2

SUPERVISION

Article 44

1. Member States shall provide that currency exchange offices and trust or company service providers shall be licensed or registered and providers of gambling services be [...] regulated.
2. Member States shall require competent authorities to ensure that the persons who hold a management function in entities referred to in paragraph 1, or are the beneficial owners of such entities, are fit and proper persons.
3. In respect of the obliged entities referred to in Article 2(1)(3) (a), (b) and (d), Member States shall ensure that competent authorities take the necessary measures to prevent [...] criminals or their associates from holding a management function in or being the beneficial owners of those obliged entities.

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 these 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.
4. Member States shall ensure that competent authorities of the Member State in which the obliged entity operates establishments supervise that these establishments respect the national provisions of that Member State pertaining to this Directive. **In the case of the establishments referred to in article 42 (8), such supervision may include the taking of appropriate and proportionate measures to address serious failings that require immediate remedies. These measures shall be temporary and be terminated when the failings identified are addressed, including, with the assistance of or in cooperation with the home country's competent authorities, in accordance with Article 42 (1a) of this Directive.**
5. Member States shall ensure that competent authorities of the Member State in which the obliged entity operates establishments 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 when applying a risk-based approach to supervision, competent authorities:
 - (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. EBA, EIOPA and ESMA shall 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 characteristics of a risk-sensitive approach to supervision and the steps to be taken 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 foreseen. These guidelines shall be issued within 2 years of the date of entry into force of this Directive.

SECTION 3

CO-OPERATION

SUBSECTION I

NATIONAL CO-OPERATION

Article 46

Member States shall ensure that policy makers, the FIUs, supervisors and other competent authorities involved in anti-money laundering and combating ~~terrorist~~ the financing of terrorism have effective mechanisms to enable them to co-operate and co-ordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing, including with a view to fulfilling their obligation under Article 7 of this Directive.

SUBSECTION II

CO-OPERATION WITH EBA, EIOPA AND ESMA

Article 47

The competent authorities shall provide EBA, EIOPA and ESMA with all the information necessary to carry out their duties under this Directive.

SUBSECTION III

CO-OPERATION BETWEEN FIUS AND WITH THE EUROPEAN COMMISSION

Article 48

The Commission may lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Union. It may regularly convene representatives from Member States' FIUs, namely in the form of the EU Financial Intelligence Units' Platform, in order to facilitate cooperation among national FIUs and exchange views on co-operation related issues such as effective international FIU co-operation, the identification of suspicious transactions with a cross-border dimension, the standardisation of reporting formats through the FIU.net network or its successor and the joint analysis of cross-border cases as well as trends and factors relevant to assessing money laundering and terrorist financing risks both on the national and supranational level.

Article 49

Member States shall ensure that their FIUs co-operate with each other to the greatest extent possible, regardless of their organisational status.

Article 50

1. Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing and the natural or legal person involved, even if the type of predicate offences possibly involved is not identified at the time of the exchange. A request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used. Different exchange mechanisms may apply if so agreed between the FIUs, in particular as regards exchanges through the decentralised computer network FIU.net or its successor.

When an FIU receives a report pursuant to Article 32(1)(a) of this Directive, which concerns another Member State, it shall promptly forward it to the FIU of that Member State.

2. Member States shall ensure that the FIU to whom the request is made is required to use the whole range of its powers which it would use domestically 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.
3. An FIU may refuse to divulge information only in exceptional circumstances where the exchange could impair fundamental national interests. These exceptions should be specified in a way which prevents misuse and undue limitations to the free exchange of information for analytical purposes.

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.

Article 52

1. Member States shall ensure that the exchanged information is used only for the purpose for which it was sought or provided and that any dissemination of the information submitted pursuant to Articles 49 and 50 by the receiving FIU to any other authority, agency or department, or any use of this information for purposes beyond those originally approved, is made subject to the prior authorisation by the FIU providing the information.
2. The requested FIU's prior consent to disseminate the information to competent authorities should be granted promptly and to the largest extent possible. The requested FIU should not refuse its consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could lead to impairment of a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State of the requested FIU, or would otherwise not be in accordance with fundamental principles of national law of that Member State. Any such refusal to grant consent shall be appropriately explained.

Article 53

1. Member States shall require their FIUs to use protected channels of communication between themselves and encourage the use of the FIU.net network or its successor.
2. Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs co-operate to apply state-of-the-art technologies. These 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.

Article 53bis

Differences between national law definitions of tax crimes should not impede the ability of FIUs to exchange information or provide assistance to another FIU based in the Union.

Article 54

deleted

SUBSECTION IV

DIAGONAL CO-OPERATION

Article 54a

deleted

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 in accordance with Articles 55 to 58.
2. Without prejudice to the right of Member States to provide for and impose criminal penalties, Member States shall lay down rules on administrative ~~penalties~~ **sanctions** and other administrative measures in respect of breaches of the national provisions transposing this Directive, and shall take all measures necessary to ensure that they are implemented. Those measures and **sanctions** ~~penalties~~ shall be effective, proportionate and dissuasive.

Where Member States decide not to lay down rules for administrative **sanctions** ~~penalties~~ for breaches which are subject to national criminal law they shall communicate to the Commission the relevant criminal law provisions.

3. Member States shall ensure that where obligations apply to legal persons in the event of a breach of national provisions transposing this Directive, ~~penalties~~ **sanctions** and measures can be applied, subject to the conditions laid down in national law, to the members of the management body and to other natural persons who under national law are responsible for the breach.
4. Member States shall ensure that the competent authorities have, in accordance with Article 45(2) and (3), all the supervisory and investigatory powers that are necessary for the exercise of their functions.

5. Competent authorities shall exercise their powers to impose ~~penalties~~ **sanctions** and measures in accordance with this Directive and with national law, in any of the following ways:
- (a) directly;
 - (b) in collaboration with other authorities;
 - (c) under their responsibility by delegation to such authorities;
 - (d) by application to the competent judicial authorities.

In the exercise of their powers to impose ~~penalties~~ **sanctions** and measures, competent authorities shall cooperate closely to ensure that administrative measures or ~~penalties~~ **sanctions** produce the desired results and coordinate their action when dealing with cross border cases.

Article 56

1. **Member States shall ensure that** ~~This Article shall at least apply~~ **at least** to situations ~~where obliged entities demonstrate serious, repetitive or systematic failings~~ **by obliged entities** in relation to the requirements of the following Articles:
- (a) 9 to 23 (customer due diligence);
 - (b) 32, 33 and 34 (suspicious transaction reporting);
 - (c) 39 (record keeping); and
 - (d) 42 and 43 (internal controls).
2. Member States shall ensure that in the cases referred to in paragraph 1, the administrative measures and **sanctions** ~~penalties~~ that can be applied to persons responsible include at least the following:
- (a) a public statement which identifies the natural or legal person responsible for the breach and the nature of the breach;
 - (b) an order requiring the natural or legal person responsible for the breach to cease the conduct and to desist from a repetition of that conduct;

- (c) where an obliged entity is subject to an authorisation, withdrawal or suspension of the authorisation;
- (d) a temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person responsible for the breach, from exercising managerial functions in obliged entities;
- (e) *deleted*
- (f) *deleted*
- (g) **maximum** administrative pecuniary **sanctions** ~~penalties of up to~~ at least twice the amount of the benefit derived from the breach where that benefit can be determined or **at least** EUR [x 000 000].

2a. Member States shall ensure that, by derogation from paragraph 2(g), where the obliged entity concerned is a credit or financial institution, also the following [...] **sanctions** ~~penalties~~ can be applied:

- (a) in the case of a legal person, **maximum** administrative pecuniary **sanctions** ~~penalties~~ of **at least EUR x 000 000 or** ~~up to~~ 10% of the total annual turnover according to the latest available accounts approved by the management body; where the obliged entity is a parent undertaking or a subsidiary of a parent undertaking which has to prepare consolidated financial accounts [as defined in Article 22 of Directive 2013/34/EU], the relevant total annual turnover shall be the total annual turnover or the corresponding type of income according to the relevant accounting Directives according to the last available consolidated accounts approved by the management body of the ultimate parent undertaking;
- (b) in the case of a natural person, **maximum** administrative pecuniary **sanctions** ~~penalties~~ of **at least** ~~up to~~ EUR 5 000 000, or in the Member States whose currency is not the euro, the corresponding value in the national currency on the date of entry into force of this Directive.

3. Member States may empower competent authorities to impose additional types of sanctions in addition to paragraph 2(a) to (d) of this Article or to impose pecuniary sanctions exceeding the amounts referred to in paragraphs 2(g) and 2a of this Article.

Article 57

1. Member States shall ensure that a decision imposing an administrative penalty or measure for breach of this Directive against which there is no appeal shall be published by competent authorities on their official website immediately after the legal or natural person sanctioned is informed of that decision. The publication shall include at least information on the type and nature of the breach and the identity of the legal or natural persons responsible. Member States are not obliged to apply the above provisions to decisions imposing measures that are of an investigatory nature.

However, where the publication of the identity of the legal persons or personal data of natural persons is considered by the competent authority to be disproportionate following a case-by-case assessment conducted on the proportionality of the publication of such data, or where publication jeopardizes the stability of financial markets or an on-going investigation, competent authorities shall either:

- (a) delay the publication of the decision to impose a sanction or a measure until the moment where the reasons for non publication cease to exist;
 - (b) publish the decision to impose a sanction or a measure on an anonymous basis in a manner which is in conformity with national law, if such anonymous publication ensures an effective protection of the personal data concerned; In the case of a decision to publish a sanction or measure on an anonymous basis the publication of the relevant data may be postponed for a reasonable period of time if it is foreseen that within that period the reasons for anonymous publication shall cease to exist.
 - (c) not publish the decision to impose a sanction or measure at all in the event that the options set out in (a) and (b) above are considered insufficient to ensure:
 - (i) that the stability of financial markets would not be put in jeopardy; or
 - (ii) the proportionality of the publication of such decisions with regard to measures which are deemed to be of a minor nature.
- 1a. Where Member States permit publication of decisions against which there is an appeal, competent authorities shall also publish, immediately, on their official website such information and any subsequent information on the outcome of such appeal. Moreover, any decision annulling a previous decision to impose a sanction or a measure shall also be published.

- 1b. Competent authorities shall ensure that any publication in accordance with this Article, shall remain on their official website for a period of five years after its publication. Personal data contained in the publication shall only be kept on the official website of the competent authority for the period which is necessary in accordance with the applicable data protection rules.
2. Member States shall ensure that when determining the type and level of administrative penalties or measures, the competent authorities shall take into account all relevant circumstances, including where appropriate:
 - (a) the gravity and the duration of the breach;
 - (b) the degree of responsibility of the responsible natural or legal person;
 - (c) the financial strength of the responsible natural or legal person, as indicated for example by the total turnover of the responsible legal person or the annual income of the responsible natural person;
 - (d) the benefit derived from the breach by the responsible natural or legal person, insofar as it can be determined;
 - (e) the losses for third parties caused by the breach, insofar as they can be determined;
 - (f) the level of cooperation of the responsible person with the competent authority
 - (g) previous breaches by the responsible natural or legal person.
3. *deleted*
4. Member States shall ensure that legal persons can be held liable for infringements referred to in paragraph 1 of Article 56 committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person based on any of the following:
 - (e) a power of representation of the legal person;
 - (f) an authority to take decisions on behalf of the legal person; or
 - (g) an authority to exercise control within the legal person.

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

Article 58

1. Member States shall ensure that competent authorities establish effective and reliable mechanisms to encourage reporting of potential or actual breaches of the national provisions transposing 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 or persons in a comparable position of obliged entities who report breaches committed within the obliged entity;
 - (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.
 - (d) clear rules that ensure that confidentiality is guaranteed in all cases in relation to the person who reports the breaches committed within the obliged entity, unless disclosure is required by national law in the context of further investigations or subsequent judicial proceedings.
3. Member States shall require obliged entities to have in place appropriate procedures for their employees or persons in a comparable position to report breaches internally through a specific, independent and anonymous channel, proportionate to the nature and size of the obliged entity concerned.

Article 58a

1. Member States shall ensure that the competent authorities inform EBA, EIOPA and ESMA of all administrative ~~penalties~~ **sanctions** and measures imposed in accordance with Articles 55 and 56 on obliged entities referred to in Article 2(1)(1) and (2), including of any appeal in relation thereto and the outcome thereof. EBA, EIOPA and ESMA shall coordinate to maintain a central database of administrative **sanctions** ~~penalties~~ and measures communicated to it solely for the purposes of exchanging information between competent authorities. That database shall be accessible to competent authorities only and it shall be updated on the basis of the information provided by competent authorities.

2. Member States shall require competent authorities when assessing the appropriateness of persons for the purposes of Article 44 to consult the database of administrative **sanctions penalties** mentioned in paragraph 1 of this Article. In the event of a change of status or a successful appeal, EBA shall delete or update relevant entries in the database on request by the competent authorities.
3. The competent authorities, in accordance with ~~Decision 2009/316/JHA, Framework Decision 2009/315/JHA and~~ their national law, shall check the existence of a relevant conviction in the criminal record of the person concerned, and exchange information. **For those purposes, information shall be exchanged in accordance with Decision 2009/316/JHA(1) and Framework Decision 2009/315/JHA(2) as implemented in national law.**
4. EBA, EIOPA and ESMA shall maintain a website with links to each competent authority's publication of administrative penalties and measures imposed in accordance with Article 57 on obliged entities referred to in Article 2(1)(1) and (2), and shall show the time period for which each Member State publishes administrative **sanctions penalties** and measures.

CHAPTER VIa

PROCESSING OF PERSONAL DATA

Article 58b

The processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC and, where relevant, with Regulation (EC) No 45/2001.

CHAPTER VII

FINAL PROVISIONS

Article 58c

1. The Commission shall be assisted by the Committee for the Prevention of Money Laundering and Terrorist Financing ('CPMLTF'), established by Directive 2005/60/EC. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time – limit for delivery of the opinion, the chair of the committee so decides or a two-thirds majority of committee members so request.

Article 59

Within four years after the date of entry into force of this Directive, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and the Council.

Article 60

Directives 2005/60/EC and 2006/70/EC are repealed with effect from [*insert date – day after the date set out in the first subparagraph of Article 61*].

References to the repealed Directives shall be construed as being made to this Directive and should be read in accordance with the correlation table 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 [*two years after adoption*] at the latest. They shall forthwith communicate to the Commission the text of those provisions.

When Member States adopt those provisions, 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.

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 Strasbourg,

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 paragraph (3).
- (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 Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions).

(3) Geographical risk factors:

- (a) other EU Member States;
- (b) third countries having effective ~~anti-money laundering/combating terrorist financing~~ AML/CFT systems;
- (c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
- (d) third countries which have requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and effectively implement those requirements.

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 (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 might favour anonymity;
 - (c) non-face-to-face business relationships or transactions;
 - (d) payment received from unknown or un-associated 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.

- (3) Geographical risk factors:
 - (a) countries identified **in accordance with Article 8a of this Directive and** by credible sources, such **as** FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, as not having effective ~~anti-money laundering/combating terrorist financing~~ **AML/CFT** systems;
 - (b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
 - (c) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;

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

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 25

Article 17	-
Article 18	Article 26
	Article 27
Article 19	Article 28
	Article 29
	Article 30
Article 20	-
Article 21	Article 31
Article 22	Article 32
Article 23	Article 33
Article 24	Article 34
Article 25	Article 35
Article 26	Article 36
Article 27	Article 37
Article 28	Article 38
Article 29	-
Article 30	Article 39
Article 31	Article 42
Article 32	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	-