DIRECTIVES

DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 May 2015

on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) Flows of illicit money can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. Money laundering, terrorism financing and organised crime remain significant problems which should be addressed at Union level. In addition to further developing the criminal law approach at Union level, targeted and proportionate prevention of the use of the financial system for the purposes of money laundering and terrorist financing is indispensable and can produce complementary results.

(2) The soundness, integrity and stability of credit institutions and financial institutions, and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin of criminal proceeds or to channel lawful or illicit money for terrorist purposes. In order to facilitate their criminal activities, money launderers and financers of terrorism could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the Union's integrated financial area entails. Therefore, certain coordinating measures are necessary at Union level. At the same time, the objectives of protecting society from crime and protecting the stability and integrity of the Union's financial system should be balanced against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs.

(3) This Directive is the fourth directive to address the threat of money laundering. Council Directive 91/308/EEC ([4]) defined money laundering in terms of drugs offences and imposed obligations solely on the financial sector.

([1]) OJ C 166, 12.6.2013, p. 2.
([2]) OJ C 271, 19.9.2013, p. 31.
([3]) Position of the European Parliament of 11 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 20 April 2015 (not yet published in the Official Journal). Position of the European Parliament of 20 May 2015 (not yet published in the Official Journal).
([4]) Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (OJ L 166, 28.6.1991, p. 77).

Directive 2001/97/EC of the European Parliament and of the Council [1] extended the scope of Directive 91/308/EEC both in terms of the crimes covered and in terms of the range of professions and activities covered. In June 2003, the Financial Action Task Force (FATF) revised its Recommendations to cover terrorist financing, and provided more detailed requirements in relation to customer identification and verification, the situations where a higher risk of money laundering or terrorist financing may justify enhanced measures and also the situations where a reduced risk may justify less rigorous controls. Those changes were reflected in Directive 2005/60/EC of the European Parliament and of the Council [2] and in Commission Directive 2006/70/EC [3].

(4) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even at Union level, without taking into account international coordination and cooperation, would have very limited effect. The measures adopted by the Union in that field should therefore be compatible with, and at least as stringent as, other actions undertaken in international fora. Union action should continue to take particular account of the FATF Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing. With a view to reinforcing the efficacy of the fight against money laundering and terrorist financing, the relevant Union legal acts should, where appropriate, be aligned with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the 'revised FATF Recommendations').

(5) Furthermore, the misuse of the financial system to channel illicit or even lawful money into terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures laid down in this Directive should address the manipulation of money derived from serious crime and 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 such cash payments, 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 should be able to adopt lower thresholds, additional general limitations to the use of cash and further stricter provisions.

(7) The use of electronic money products is increasingly considered to be a substitute for bank accounts, which, in addition to the measures laid down in Directive 2009/110/EC of the European Parliament and of the Council [4], justifies subjecting those products to anti-money laundering and countering the financing of terrorism (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 of the beneficial owner, but not from the monitoring of transactions or of business relationships. The risk-mitigating conditions should include a requirement that exempt electronic money products 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. Such an exemption should be 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 15.

(8) As concerns the obliged entities which are subject to this Directive, estate agents could be understood to include letting agents, where applicable.

---

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

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

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

[4] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

(9) Legal professionals, as defined by the Member States, should be subject to this Directive when participating in financial or corporate transactions, including when 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 before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Therefore, legal advice should remain subject to the obligation of professional secrecy, except where the legal professional is taking part in money laundering or terrorist financing, the legal advice is provided for the purposes of money laundering or terrorist financing, or the legal professional knows that the client is seeking legal advice for the purposes of money laundering or terrorist financing.

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

(11) It is important expressly to highlight that 'tax crimes' relating to direct and indirect taxes are included in the broad definition of 'criminal activity' in this Directive, in line with the revised FATF Recommendations. Given that different tax offences may be designated in each Member State as constituting 'criminal activity' punishable by means of the sanctions as referred to in point (4)(f) of Article 3 of this Directive, national law definitions of tax crimes may diverge. While no harmonisation of the definitions of tax crimes in Member States' national law is sought, Member States should allow, to the greatest extent possible under their national law, the exchange of information or the provision of assistance between EU Financial Intelligence Units (FIUs).

(12) 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 does not automatically result in finding the beneficial owner, it should be one evidential factor among others to be taken into account. Member States should be able, however, to decide that a lower percentage may be an indication of ownership or control.

(13) 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 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 purpose of preparing consolidated financial statements, such as through a 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 ultimately owns or 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, may consider the senior managing official(s) to be the beneficial owner(s).

(14) 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 entities incorporated within their territory in accordance with national law obtain and hold adequate, accurate and current information on their beneficial ownership, in addition to basic information such as the company name and address and proof of incorporation and legal ownership. With a view to enhancing transparency in order to combat the misuse of legal entities, Member States should ensure that beneficial ownership information is stored in a central register located outside the company, in full compliance with Union law. Member States can, for that purpose, use a central database which collects beneficial ownership information, or the business register, or another central register. Member States may decide that obliged entities are responsible for filling in the register. Member States should make sure that in all cases that information is made available to competent authorities and FIUs and is provided to obliged entities when the latter take customer due diligence measures. Member States should also ensure that other persons who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as corruption, tax

crimes and fraud, are granted access to beneficial ownership information, in accordance with data protection rules. The persons who are able to demonstrate a legitimate interest should have access to information on the nature and extent of the beneficial interest held consisting of its approximate weight.

(15) For that purpose, Member States should be able, under national law, to allow for access that is wider than the access provided for under this Directive.

(16) Timely access to information on beneficial ownership should be ensured in ways which avoid any risk of tipping off the company concerned.

(17) In order to ensure a level playing field among the different types of legal forms, trustees should also be required to obtain, hold and provide beneficial ownership information to obliged entities taking customer due diligence measures and to communicate that information to a central register or a central database and they should disclose their status to obliged entities. Legal entities such as foundations and legal arrangements similar to trusts should be subject to equivalent requirements.

(18) This Directive should also apply to activities of obliged entities which are performed on the internet.

(19) New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering.

(20) The representatives of the Union in the governing bodies of the European Bank for Reconstruction and Development are encouraged to implement this Directive and to publish on its website AML/CFT policies, containing detailed procedures that would give effect to this Directive.

(21) The use of gambling sector services to launder the proceeds of criminal activity is of concern. In order to mitigate the risks relating to gambling services, this Directive should provide for an obligation for providers of gambling services posing higher risks to apply customer due diligence measures for single transactions amounting to EUR 2 000 or more. Member States should ensure that obliged entities apply the same threshold to the collection of winnings, wagering a stake, including by the purchase and exchange of gambling chips, or both. Providers of gambling services with physical premises, such as 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 requirements laid down in this Directive. The use of an exemption by a Member State should be considered only in strictly limited and justified circumstances, and where the risks of money laundering or terrorist financing are low. Such exemptions should be subject to a specific risk assessment which also considers the degree of vulnerability of the applicable transactions. They should be notified to the Commission. In the risk assessment, Member States should indicate how they have taken into account any relevant findings in the reports issued by the Commission in the framework of the supranational risk assessment.

(22) The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, 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 in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively.

(23) Underpinning the risk-based approach is the need for Member States and the Union to identify, understand and mitigate the risks of money laundering and terrorist financing that they face. The importance of a supranational approach to risk identification has been recognised at international level, and the European Supervisory Authority (European Banking Authority) (EBA), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([1]), the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (EIOPA), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council ([2]), and the European Supervisory Authority (European Securities and Markets Authority) (ESMA),

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

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

established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([1]), should be tasked with issuing an opinion, through their Joint Committee, on the risks affecting the Union financial sector.

(24) The Commission is well placed to review specific cross-border threats that could affect the internal market and that cannot be identified and effectively combatted by individual Member States. It should therefore be entrusted with the responsibility for coordinating the assessment of risks relating to cross-border activities. Involvement of the relevant experts, such as the Expert Group on Money Laundering and Terrorist Financing and the representatives from the FIUs, as well as, where appropriate, from other Union-level bodies, is essential for the effectiveness of that process. National risk assessments and experience are also an important source of information for the process. Such assessment of the cross-border risks by the Commission should not involve the processing of personal data. In any event, data should be fully anonymised. National and Union data protection supervisory authorities should be involved only if the assessment of the risk of money laundering and terrorist financing has an impact on the privacy and data protection of individuals.

(25) The results of risk assessments should, where appropriate, be made available to obliged entities in a timely manner to enable them to identify, understand, manage and mitigate their own risks.

(26) In addition, to identify, understand, manage and mitigate risks at Union level to an even greater degree, Member States should make available the results of their risk assessments to each other, to the Commission and to EBA, EIOPA and ESMA (the 'ESAs').

(27) When applying this Directive, it is appropriate to take account of the characteristics and needs of smaller obliged entities which fall under its scope, and to ensure treatment which is appropriate to their specific needs, and the nature of the business.

(28) In order to protect the proper functioning of the Union financial system and of the internal market from money laundering and terrorist financing, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission in order to identify third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes ('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 address efficiently 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 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.

(29) Member States should at least provide for enhanced customer due diligence measures to be applied by the obliged entities when dealing with natural persons or legal entities established in high-risk third countries identified by the Commission. Reliance on third parties established in such high-risk third countries should also be prohibited. Countries not included in the list should not be automatically considered to have effective AML/CFT systems and natural persons or legal entities established in such countries should be assessed on a risk-sensitive basis.

(30) Risk itself is variable in nature, and the variables, 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. Therefore, there are circumstances in which enhanced due diligence should be applied and others in which simplified due diligence may be appropriate.

(31) 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 in which particularly rigorous customer identification and verification procedures are required.

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

(32) This is particularly true of relationships with individuals who hold or who have held important public functions, within the Union or internationally, and particularly individuals 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 particular attention to such persons and to apply appropriate enhanced customer due diligence measures with respect to persons who are or who have been entrusted with prominent public functions domestically or abroad and with respect to senior figures in international organisations.

(33) The requirements relating to politically exposed persons are of a preventive and not criminal nature, and should not be interpreted as stigmatising politically exposed persons as being involved in criminal activity. Refusing a business relationship with a person simply on the basis of the determination that he or she is a politically exposed person is contrary to the letter and spirit of this Directive and of the revised FATF Recommendations.

(34) Obtaining approval from senior management for establishing business relationships does not need to imply, in all cases, obtaining approval from the board of directors. It should be possible for such approval to be granted by someone with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and of sufficient seniority to take decisions affecting its risk exposure.

(35) 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 customer due diligence should remain with the obliged entity to which the customer is introduced. The third party, or the person that has introduced the customer, should also retain its own responsibility for compliance with this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that it has a relationship with the customer that is covered by this Directive.

(36) In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external persons not covered by this Directive, any AML/CFT obligations upon those agents or outsourcing service providers as part of the obliged entities could arise only from the contract between the parties and not from this Directive. Therefore the responsibility for complying with this Directive should remain primarily with the obliged entity.

(37) All Member States have, or should, set up operationally independent and autonomous 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. An operationally independent and autonomous FIU should mean that the FIU has the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and disseminate specific information. Suspicious transactions and other information relevant to money laundering, associated predicate offences and terrorist financing should be reported to the FIU, which should serve as a central national unit for receiving, analysing and disseminating to the competent authorities the results of its analyses. All suspicious transactions, including attempted transactions, should be reported, regardless of the amount of the transaction. Reported information could also include threshold-based information.

(38) By way of derogation from the general prohibition against carrying out suspicious transactions, obliged entities should be able to carry out suspicious transactions before informing the competent authorities where refraining from such carrying out 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.

(39) For certain obliged entities, Member States should have the possibility to designate an appropriate self-regulatory body as the authority to be informed in the first instance instead of the FIU. In accordance 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 for upholding the protection of fundamental rights as concerns the reporting obligations applicable to lawyers. Member States should provide for the means and manner by which to achieve the protection of professional secrecy, confidentiality and privacy.

(40) Where a Member State decides to designate such a self-regulatory body, it may allow or require that body not to transmit to the FIU any information obtained from persons represented by that body where such information has

been received from, or obtained on, one of their clients, in the course of ascertaining the legal position of their client, or in performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

(41) There have been a number of cases where employees who have reported their suspicions of money laundering have been subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, it is crucial that this issue be addressed to ensure effectiveness of the AML/CFT system. Member States should be aware of this problem and should do whatever they can to protect individuals, including employees and representatives of the obliged entity, from such threats or hostile action, and to provide, in accordance with national law, appropriate protection to such persons, particularly with regard to their right to the protection of their personal data and their rights to effective judicial protection and representation.

(42) Directive 95/46/EC of the European Parliament and of the Council ([1]), as transposed into national law, applies to the processing of personal data for the purposes of this Directive. Regulation (EC) No 45/2001 of the European Parliament and of the Council ([2]) applies to the processing of personal data by the Union institutions and bodies for the purposes of this Directive. The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States. This Directive is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including Council Framework Decision 2008/977/JHA ([3]), as implemented in national law.

(43) It is essential that the alignment of this Directive with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter. Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Directive, and for the activities required under this Directive such as carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of this Directive and personal data should not be further processed in a way that is incompatible with that purpose. In particular, further processing of personal data for commercial purposes should be strictly prohibited.

(44) The revised FATF Recommendations demonstrate that, in order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. In order to avoid different approaches and in order to fulfil the requirements relating to the protection of personal data and legal certainty, that retention period should be fixed at five years after the end of a business relationship or of an occasional transaction. However, if necessary for the purposes of prevention, detection or investigation of money laundering and terrorist financing, and after carrying out an assessment of the necessity and proportionality, Member States should be able to allow or require the further retention of records for a period not exceeding an additional five years, without prejudice to the national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings. Member States should require that specific safeguards be put in place to ensure the security of data and should determine which persons, categories of persons or authorities should have exclusive access to the data retained.

(45) For the purpose of ensuring the appropriate and efficient administration of justice during the period for transposition of this Directive into the Member States' national legal orders, and in order to allow for its smooth interaction with national procedural law, information and documents pertinent to ongoing legal proceedings for

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

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

([3]) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

the purpose of the prevention, detection or investigation of possible money laundering or terrorist financing, which have been pending in the Member States on the date of entry into force of this Directive, should be retained for a period of five years after that date, and it should be possible to extend that period for a further five years.

(46) The rights of access to data by the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Exceptions to and restrictions of that right in accordance with Article 13 of Directive 95/46/EC and, where relevant, Article 20 of Regulation (EC) No 45/2001, may therefore be justified. The data subject has the right to request that a supervisory authority referred to in Article 28 of Directive 95/46/EC or, where applicable, the European Data Protection Supervisor, check the lawfulness of the processing and has the right to seek a judicial remedy referred to in Article 22 of that Directive. The supervisory authority referred to in Article 28 of Directive 95/46/EC may also act on an *ex-officio* basis. Without prejudice to the restrictions to the right to access, the supervisory authority should be able to inform the data subject that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.

(47) Persons that merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution and persons that provide credit institutions or financial institutions solely with messaging or other support systems for transmitting funds or with clearing and settlement systems do not fall within the scope of this Directive.

(48) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Union credit institutions and financial institutions have branches and subsidiaries located in third countries in which the requirements in that area are less strict than those of the Member State, they should, in order to avoid the application of very different standards within the institution or group of institutions, apply to those branches and subsidiaries Union standards or notify the competent authorities of the home Member State if the application of such standards is not possible.

(49) Feedback on the usefulness and follow-up of the suspicious transactions reports they present should, where practicable, be made available to obliged entities. To make this possible, and to be able to review the effectiveness of their systems for combating money laundering and terrorist financing, Member States should maintain, and improve the quality of, relevant statistics. To further enhance the quality and consistency of the statistical data collected at Union level, the Commission should keep track of the Union-wide situation with respect to the fight against money laundering and terrorist financing and should publish regular overviews.

(50) Where Member States require issuers of electronic money and payment service providers which are established in their territory in forms other than a branch and the head office of which is situated in another Member State, to appoint a central contact point in their territory, they should be able to require that such a central contact point, acting on behalf of the appointing institution, ensure the establishments' compliance with AML/CFT rules. They should also ensure that that requirement is proportionate and does not go beyond what is necessary to achieve the aim of compliance with AML/CFT rules, including by facilitating the respective supervision.

(51) Competent authorities should ensure that, with regard to currency exchange offices, cheque cashing offices, trust or 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. 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.

(52) Where an obliged entity operates establishments in another Member State, including through a network of agents, the competent authority of the home Member State should be responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures. This could involve on-site visits in establishments based in another Member State. The competent authority of the home Member State should cooperate closely with the competent authority of the host Member State and should inform the latter of any issues that could affect their assessment of the establishment's compliance with the host AML/CFT rules.

(53) Where an obliged entity operates establishments in another Member State, including through a network of agents or persons distributing electronic money in accordance with Article 3(4) of Directive 2009/110/EC, the competent authority of the host Member State retains responsibility for enforcing the establishment's compliance with AML/CFT rules, including, where appropriate, by carrying out onsite inspections and offsite monitoring and by taking appropriate and proportionate measures to address serious infringements of those requirements. The competent authority of the host Member State should cooperate closely with the competent authority of the home Member State and should inform the latter of any issues that could affect its assessment of the obliged entity's application of group AML/CFT policies and procedures. In order to remove serious infringements of AML/CFT rules that require immediate remedies, the competent authority of the host Member State should be able 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 competent authority of the home Member State.

(54) Taking into account the transnational nature of money laundering and terrorist financing, coordination and cooperation between FIUs are extremely important. In order to improve such coordination and cooperation, and, in particular, to ensure that suspicious transaction reports reach the FIU of the Member State where the report would be of most use, detailed rules are laid down in this Directive.

(55) The EU Financial Intelligence Units' Platform (the 'EU FIUs Platform'), an informal group composed of representatives from FIUs and active since 2006, is used to facilitate cooperation among FIUs and exchange views on cooperation-related issues such as effective cooperation among FIUs and between FIUs and third-country financial intelligence units, joint analysis of cross-border cases and trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

(56) Improving the exchange of information between FIUs within the Union is particularly important in addressing the transnational character of money laundering and terrorist financing. The use of secure facilities for the exchange of information, in particular the decentralised computer network FIU.net (the 'FIU.net') or its successor and the techniques offered by FIU.net, should be encouraged by Member States. The initial exchange of information between FIUs relating to money laundering or terrorist financing for analytical purposes which is not further processed or disseminated should be permitted unless such exchange of information would be contrary to fundamental principles of national law. The exchange of information on cases identified by FIUs as possibly involving tax crimes should be without prejudice to the exchange of information in the field of taxation in accordance with Council Directive 2011/16/EU [1] or in accordance with international standards on the exchange of information and administrative cooperation in tax matters.

(57) 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 persons. In accordance with Union and national law, 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 without prejudice to judicial authorisation where applicable. Member States could also consider establishing mechanisms to ensure that competent authorities have procedures in place to identify assets without prior notification to the owner.

(58) Member States should encourage their competent authorities to provide rapidly, constructively and effectively the widest range of cross-border cooperation for the purposes of this Directive, without prejudice to any rules or procedures applicable to judicial cooperation in criminal matters. Member States should in particular ensure that their FIUs exchange information freely, spontaneously or upon request, with third-country financial intelligence units, having regard to Union law and to the principles relating to information exchange developed by the Egmont Group of Financial Intelligence Units.

(59) The importance of combating money laundering and terrorist financing should result in Member States laying down effective, proportionate and dissuasive administrative sanctions and measures in national law for failure to respect the national provisions transposing this Directive. Member States currently have a diverse range of administrative sanctions and measures for breaches of the key preventative provisions in place. That diversity could be detrimental to the efforts made in combating money laundering and terrorist financing and the Union's

[1] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ L 64, 11.3.2011, p. 1).

response is at risk of being fragmented. This Directive should therefore provide for a range of administrative sanctions and measures by Member States at least for serious, repeated or systematic breaches of the requirements relating to customer due diligence measures, record-keeping, reporting of suspicious transactions and internal controls of obliged entities. The range of sanctions and measures should be sufficiently broad to allow Member States and competent authorities to take account of the differences between obliged entities, in particular between credit institutions and financial institutions and other obliged entities, as regards their size, characteristics and the nature of the business. In transposing this Directive, Member States should ensure that the imposition of administrative sanctions and measures in accordance with this Directive, and of criminal sanctions in accordance with national law, does not breach the principle of *ne bis in idem*.

(60) For the purposes of assessing the appropriateness of persons holding a management function in, or otherwise controlling, obliged entities, any exchange of information about criminal convictions should be carried out in accordance with Council Framework Decision 2009/315/JHA ([1]) and Council Decision 2009/316/JHA ([2]), as transposed into national law, and with other relevant provisions of national law.

(61) Regulatory technical standards in financial services should ensure consistent harmonisation and adequate protection of depositors, investors and consumers across the Union. As bodies with highly specialised expertise, it would be efficient and appropriate to entrust the ESAs with the elaboration, for submission to the Commission, of draft regulatory technical standards which do not involve policy choices.

(62) The Commission should adopt the draft regulatory technical standards developed by the ESAs pursuant to this Directive by means of delegated acts pursuant to Article 290 TFEU and in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

(63) Given the very substantial amendments that would need to be made to Directives 2005/60/EC and 2006/70/EC in light of this Directive, they should be merged and replaced for reasons of clarity and consistency.

(64) Since the objective of this Directive, namely the protection of the financial system by means of prevention, detection and investigation of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States, as individual measures adopted by Member States to protect their financial systems could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Union public policy, but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(65) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the 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, the presumption of innocence and the rights of the defence.

(66) In accordance with Article 21 of the Charter, which prohibits discrimination based on any ground, Member States are to ensure that this Directive is implemented, as regards risk assessments in the context of customer due diligence, without discrimination.

(67) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents ([3]), 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.

(68) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 4 July 2013 ([4]),

([1]) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).
([2]) Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).
([3]) OJ C 369, 17.12.2011, p. 14.
([4]) OJ C 32, 4.2.2014, p. 9.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

SECTION 1

Subject-matter, scope and definitions

Article 1

1. This Directive aims to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing.

2. Member States shall ensure that money laundering and terrorist financing are prohibited.

3. 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 an activity to evade the legal consequences of that person's 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 an 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 an 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).

4. 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.

5. 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 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 ([1]).

6. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 3 and 5 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 natural or legal persons acting in the exercise of their professional activities:

  (a) auditors, external accountants and tax advisors;

  (b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

    (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;

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

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

(v) creation, operation or management of trusts, companies, foundations, or similar structures;

(c) trust or company service providers not already covered under point (a) or (b);

(d) estate agents;

(e) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(f) providers of gambling services.

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

Among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

In their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission pursuant to Article 6.

Any decision taken by a Member State pursuant to the first subparagraph shall be notified to the Commission, together with a justification based on the specific risk assessment. The Commission shall communicate that decision to the other Member States.

3. Member States may decide that persons that engage in a financial activity on an occasional or very limited basis where there is little risk of money laundering or terrorist financing do not fall within the scope of this Directive, provided that all of the following criteria are met:

(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 of such persons;

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

(e) the main activity of such persons is not an activity referred to in points (a) to (d) or point (f) of paragraph 1(3);

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

The first subparagraph shall not apply to persons engaged in the activity of money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC of the European Parliament and of the Council ([1]).

4. For the purposes of point (a) of paragraph 3, Member States shall require that the total turnover of the financial activity does not exceed a threshold which must be sufficiently low. That threshold shall be established at national level, depending on the type of financial activity.

5. For the purposes of point (b) of paragraph 3, Member States shall apply a maximum threshold per customer and per single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked. That maximum 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 money laundering or terrorist financing, and shall not exceed EUR 1 000.

6. For the purposes of point (c) of paragraph 3, Member States shall require that the turnover of the financial activity does not exceed 5 % of the total turnover of the natural or legal person concerned.

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

7. In assessing the risk of money laundering or terrorist financing for the purposes of this Article, Member States shall pay particular attention to any financial activity which is considered to be particularly likely, by its nature, to be used or abused for the purposes of money laundering or terrorist financing.

8. Decisions taken by Member States pursuant to paragraph 3 shall state the reasons on which they are based. Member States may decide to withdraw such decisions where circumstances change. They shall notify such decisions to the Commission. The Commission shall communicate such decisions to the other Member States.

9. Member States shall establish risk-based monitoring activities or take 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 apply:

(1) 'credit institution' means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council [1], including branches thereof, as defined in point (17) of Article 4(1) of that Regulation, located in the Union, whether its head office is situated within the Union or in a third country;

(2) 'financial institution' means:

(a) an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council [2], including the activities of currency exchange offices (bureaux de change);

(b) an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC of the European Parliament and of the Council [3], insofar as it carries out life assurance activities covered by that Directive;

(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 [4];

(d) a collective investment undertaking marketing its units or shares;

(e) an insurance intermediary as defined in point (5) of Article 2 of Directive 2002/92/EC of the European Parliament and of the Council [5] where it acts with respect to life insurance and other investment-related services, with the exception of a tied insurance intermediary as defined in point (7) of that Article;

(f) branches, when located in the Union, of financial institutions as referred to in points (a) to (e), whether their head office is situated in a Member State or in a third country;

(3) 'property' means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) 'criminal activity' means any kind of criminal involvement in the commission of the following serious crimes:

(a) acts set out in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(b) any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;

---

[1] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

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

[3] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

[4] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ L 145, 30.4.2004, p. 1).

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

(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA ([1]);

(d) fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1(1) and Article 2(1) of the Convention on the protection of the European Communities' financial interests ([2]);

(e) corruption;

(f) all offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national law of the Member States, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that 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;

(5) 'self-regulatory body' means a body that represents members of a profession and has a role in regulating them, in performing certain supervisory or monitoring type functions and in ensuring the enforcement of the rules relating to them;

(6) '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 and includes at least:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control. Control through other means may 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 ([3]);

(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), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point;

(b) in the case of trusts:

(i) the settlor;

(ii) the trustee(s);

(iii) the protector, if any;

(iv) the beneficiaries, or where the individuals benefiting 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 by means of direct or indirect ownership or by other means;

([1]) Joint Action 98/733/JHA of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (OJ L 351, 29.12.1998, p. 1).

([2]) OJ C 316, 27.11.1995, p. 49.

([3]) Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

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

(7) 'trust or company service provider' means any person that, by way of its business, provides any of the following services to third parties:

(a) the formation of 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 accordance with Union law or subject to equivalent international standards;

(8) 'correspondent relationship' means:

(a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

(b) the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers;

(9) 'politically exposed person' means a natural person who is or who has been entrusted with prominent public functions and includes the following:

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

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

(c) members of the governing bodies of political parties;

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

(e) members of courts of auditors or of the boards of central banks;

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

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

(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

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

(10) 'family members' includes the following:

(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

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

(c) the parents of a politically exposed person;

(11) 'persons known to be close associates' means:

(a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;

(b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

(12) '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 take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors;

(13) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration;

(14) 'gambling services' means a 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;

(15) '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;

(16) 'electronic money' means electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC;

(17) 'shell bank' means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, 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.

Article 4

1. Member States shall, in accordance with the risk-based approach, ensure that the scope of this Directive is 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 the purposes of money laundering or terrorist financing.

2. Where a Member State extends the scope of this Directive to professions or to categories of undertaking other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing, within the limits of Union law.

SECTION 2

Risk assessment

Article 6

1. The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.

To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate.

2. The report referred to in paragraph 1 shall cover at least the following:

(a) the areas of the internal market that are at greatest risk;

(b) the risks associated with each relevant sector;

(c) the most widespread means used by criminals by which to launder illicit proceeds.

3. The Commission shall make the report referred to in paragraph 1 available to the Member States and obliged entities in order to assist them to identify, understand, manage and mitigate the risk of money laundering and terrorist financing, and to allow other stakeholders, including national legislators, the European Parliament, the ESAs, and representatives from FIUs to better understand the risks.

4. The Commission shall make recommendations to Member States on the measures suitable for addressing the identified risks. In the event that 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.

5. By 26 December 2016, the ESAs, through the Joint Committee, shall issue an opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector (the 'joint opinion'). Thereafter, the ESAs, through the Joint Committee, shall issue an opinion every two years.

6. In conducting the assessment referred to in paragraph 1, the Commission shall organise the work at Union level, shall take into account the joint opinions referred to in paragraph 5 and shall involve the Member States' experts in the area of AML/CFT, representatives from FIUs and other Union level bodies where appropriate. The Commission shall make the joint opinions available to the Member States and obliged entities in order to assist them to identify, manage and mitigate the risk of money laundering and terrorist financing.

7. Every two years, or more frequently if appropriate, the Commission shall submit a report to the European Parliament and to the Council on the findings resulting from the regular risk assessments and the action taken based on those findings.

Article 7

1. Each Member State shall take appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it, as well as any data protection concerns in that regard. It shall keep that risk assessment up to date.

2. Each Member State shall designate an authority or establish a mechanism by which to coordinate 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, the ESAs, and other Member States.

3. In carrying out the risk assessments referred to in paragraph 1 of this Article, Member States shall make use of the findings of the report referred to in Article 6(1).

4. As regards the risk assessment referred to in paragraph 1, each Member State shall:

(a) use it to improve its AML/CFT regime, in particular by identifying any areas where obliged entities are to apply enhanced measures and, where appropriate, specifying the measures to be taken;

(b) identify, where appropriate, sectors or areas of lower or greater risk of money laundering and terrorist financing;

(c) use it to assist it in the allocation and prioritisation of resources to combat money laundering and terrorist financing;

(d) use it to ensure that appropriate rules are drawn up for each sector or area, in accordance with the risks of money laundering and terrorist financing;

(e) make appropriate information available promptly to obliged entities to facilitate the carrying out of their own money laundering and terrorist financing risk assessments.

5. Member States shall make the results of their risk assessments available to the Commission, the ESAs and the other Member States.

Article 8

1. Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities.

2. The risk assessments referred to in paragraph 1 shall be documented, kept up-to-date and made available to the relevant competent authorities and self-regulatory bodies concerned. Competent authorities may decide that individual documented risk assessments are not required where the specific risks inherent in the sector are clear and understood.

3. Member States shall ensure that obliged entities have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity. Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entities.

4. The policies, controls and procedures referred to in paragraph 3 shall include:

(a) the development of internal policies, controls and procedures, including model risk management practices, customer due diligence, reporting, record-keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening;

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

5. Member States shall require obliged entities to obtain approval from their senior management for the policies, controls and procedures that they put in place and to monitor and enhance the measures taken, where appropriate.

SECTION 3

Third-country policy

Article 9

1. Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union ('high-risk third countries') shall be identified in order to protect the proper functioning of the internal market.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 64 in order to identify high-risk third countries, taking into account strategic deficiencies, in particular in relation to:

(a) the legal and institutional AML/CFT framework of the third country, in particular:

  (i) criminalisation of money laundering and terrorist financing;

  (ii) measures relating to customer due diligence;

  (iii) requirements relating to record-keeping; and

  (iv) requirements to report suspicious transactions;

(b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing;

(c) the effectiveness of the AML/CFT system in addressing money laundering or terrorist financing risks of the third country.

3. The delegated acts referred to in paragraph 2 shall be adopted within one month after the identification of the strategic deficiencies referred to in that paragraph.

4. The Commission shall take into account, as appropriate, when drawing up the delegated acts referred to in paragraph 2, relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, in relation to the risks posed by individual third countries.

CHAPTER II

CUSTOMER DUE DILIGENCE

SECTION 1

General provisions

Article 10

1. Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts or anonymous passbooks. Member States shall, in any event, require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be subject to customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

2. Member States shall take measures to prevent misuse of bearer shares and bearer share warrants.

Article 11

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

(a) when establishing a business relationship;

(b) when carrying out an occasional transaction that:

(i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or

(ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council [1], exceeding EUR 1 000;

(c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(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 12

1. By way of derogation from points (a), (b) and (c) of the first subparagraph of Article 13(1) and Article 14, and based on an appropriate risk assessment which demonstrates a low risk, a Member State may allow obliged entities not to apply certain customer due diligence measures with respect to electronic money, where all of the following risk-mitigating conditions are met:

(a) the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 250 which can be used only in that Member State;

(b) the maximum amount stored electronically does not exceed EUR 250;

---

[1] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (see page 1 of this Official Journal).

(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.

For the purposes of point (b) of the first subparagraph, a Member State may increase the maximum amount to EUR 500 for payment instruments that can be used only in that Member State.

2. Member States shall ensure that the derogation provided for in paragraph 1 is not applicable in the case of redemption in cash or cash withdrawal of the monetary value of the electronic money where the amount redeemed exceeds EUR 100.

Article 13

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 that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations 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 obliged entity'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.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements laid down in paragraph 1. However, 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 the risks of money laundering and terrorist financing.

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, in addition to the customer due diligence measures required for the customer and the beneficial owner, credit institutions and financial institutions conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment-related insurance policies, as soon as the beneficiaries are identified or designated:

(a) in the case of beneficiaries that are identified as specifically named persons or legal arrangements, taking the name of the person;

(b) in the case of beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the credit institutions or financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

With regard to points (a) and (b) of the first subparagraph, the verification of the identity of the beneficiaries shall take place at the time of the payout. In the case of assignment, in whole or in part, of the life or other investment-related insurance to a third party, credit institutions and financial institutions aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for its own benefit the value of the policy assigned.

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

Article 14

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

3. By way of derogation from paragraph 1, Member States may allow the opening of an account with a credit institution 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 the customer due diligence requirements laid down in points (a) and (b) of the first subparagraph of Article 13(1) is obtained.

4. Member States shall require that, where an obliged entity is unable to comply with the customer due diligence requirements laid down in point (a), (b) or (c) of the first subparagraph of Article 13(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 relation to the customer in accordance with Article 33.

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 those persons ascertain the legal position of their client, or perform the task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.

5. Member States shall require that obliged entities apply the customer due diligence measures 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 15

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 business relationship or the transaction presents a lower degree of risk.

3. Member States shall ensure that obliged entities carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

Article 16

When assessing the risks of money laundering and terrorist financing relating to types of customers, 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 17

By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities and the credit institutions and financial institutions in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010, and (EU) No 1095/2010 on the risk factors to be taken into consideration and the measures to be taken in situations where simplified customer 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 shall be laid down.

SECTION 3

Enhanced customer due diligence

Article 18

1. In the cases referred to in Articles 19 to 24, and when dealing with natural persons or legal entities established in the third countries identified by the Commission as high-risk third countries, as well as in other cases of higher risk that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

Enhanced customer due diligence measures need not be invoked automatically with respect to branches or majority-owned subsidiaries of obliged entities established in the Union which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45. Member States shall ensure that those 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 and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, obliged entities 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 risks of money laundering and terrorist financing, Member States and obliged entities shall take into account at least the factors of potentially higher-risk situations set out in Annex III.

4. By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities and the credit institutions and financial institutions, in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010, and (EU) No 1095/2010 on the risk factors to be taken into consideration and the measures to be taken in situations where enhanced customer 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 shall be laid down.

Article 19

With respect to cross-border correspondent relationships with a third-country respondent institution, Member States shall, in addition to the customer due diligence measures laid down in Article 13, require their credit institutions and financial institutions to:

(a) gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution's 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 institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent institution, and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

Article 20

With respect to transactions or business relationships with politically exposed persons, Member States shall, in addition to the customer due diligence measures laid down in Article 13, require obliged entities to:

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

(b) apply the following measures in cases of business relationships with politically exposed persons:

(i) obtain senior management approval for establishing or continuing business relationships with such persons;

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

(iii) conduct enhanced, ongoing monitoring of those business relationships.

Article 21

Member States shall require obliged entities to 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 no later than at the time of the payout or at the time of the assignment, in whole or in part, of the policy. Where there are higher risks identified, in addition to applying the customer due diligence measures laid down in Article 13, Member States shall require obliged entities to:

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

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

Article 22

Where a politically exposed person is no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function by an international organisation, obliged entities shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

Article 23

The measures referred to in Articles 20 and 21 shall also apply to family members or persons known to be close associates of politically exposed persons.

Article 24

Member States shall prohibit credit institutions and financial institutions from entering into, or continuing, a correspondent relationship with a shell bank. They shall require that those institutions take appropriate measures to ensure that they do not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank.

SECTION 4

Performance by third parties

Article 25

Member States may permit obliged entities to rely on third parties to meet the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1). However, the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party.

Article 26

1. For the purposes of this Section, 'third parties' means obliged entities listed in Article 2, the member organisations or federations of those obliged entities, or other institutions or persons situated in a Member State or third country that:

(a) apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this Directive; and

(b) have their compliance with the requirements of this Directive supervised in a manner consistent with Section 2 of Chapter VI.

2. Member States shall prohibit obliged entities from relying on third parties established in high-risk third countries. Member States may exempt branches and majority-owned subsidiaries of obliged entities established in the Union from that prohibition where those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45.

Article 27

1. Member States shall ensure that obliged entities obtain from the third party relied upon the necessary information concerning the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1).

2. Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner.

Article 28

Member States shall ensure that the competent authority of the home Member State (for group-wide policies and procedures) and the competent authority of the host Member State (for branches and subsidiaries) may consider an obliged entity to comply with the provisions adopted pursuant to Articles 26 and 27 through its group programme, where all of the following conditions are met:

(a) the 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 the requirements referred to in point (b) is supervised at group level by a competent authority of the home Member State or of the third country.

Article 29

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 30

1. Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held.

Member States shall ensure that those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Chapter II.

2. Member States shall require that the information referred to in paragraph 1 can be accessed in a timely manner by competent authorities and FIUs.

3. Member States shall ensure that the information referred to in paragraph 1 is held in a central register in each Member State, for example a commercial register, companies register as referred to in Article 3 of Directive 2009/101/EC of the European Parliament and of the Council ([1]), or a public register. Member States shall notify to the Commission the characteristics of those national mechanisms. The information on beneficial ownership contained in that database may be collected in accordance with national systems.

4. Member States shall require that the information held in the central register referred to in paragraph 3 is adequate, accurate and current.

5. Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;

(c) any person or organisation that can demonstrate a legitimate interest.

The persons or organisations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held.

For the purposes of this paragraph, access to the information on beneficial ownership shall be in accordance with data protection rules and may be subject to online registration and to the payment of a fee. The fees charged for obtaining the information shall not exceed the administrative costs thereof.

6. The central register referred to in paragraph 3 shall ensure timely and unrestricted access by competent authorities and FIUs, without alerting the entity concerned. It shall also allow timely access by obliged entities when taking customer due diligence measures.

7. Member States shall ensure that competent authorities and FIUs are able to provide the information referred to in paragraphs 1 and 3 to the competent authorities and to the FIUs of other Member States in a timely manner.

8. Member States shall require that obliged entities do not rely exclusively on the central register referred to in paragraph 3 to fulfil their customer due diligence requirements in accordance with Chapter II. Those requirements shall be fulfilled by using a risk-based approach.

9. Member States may provide for an exemption to the access referred to in points (b) and (c) of paragraph 5 to all or part of the information on the beneficial ownership on a case-by-case basis in exceptional circumstances, where such access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation, or where the beneficial owner is a minor or otherwise incapable. Exemptions granted pursuant to this paragraph shall not apply to the credit institutions and financial institutions, and to obliged entities referred to in point (3)(b) of Article 2(1) that are public officials.

10. By 26 June 2019, the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring the safe and efficient interconnection of the central registers referred to in paragraph 3 via the European central platform established by Article 4a(1) of Directive 2009/101/EC. Where appropriate, that report shall be accompanied by a legislative proposal.

Article 31

1. Member States shall require that trustees of any express trust governed under their law obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust. That information shall include the identity of:

(a) the settlor;

(b) the trustee(s);

(c) the protector (if any);

([1]) Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ L 258, 1.10.2009, p. 11).

(d) the beneficiaries or class of beneficiaries; and

(e) any other natural person exercising effective control over the trust.

2. Member States shall ensure that trustees disclose their status and provide the information referred to in paragraph 1 to obliged entities in a timely manner where, as a trustee, the trustee forms a business relationship or carries out an occasional transaction above the thresholds set out in points (b), (c) and (d) of Article 11.

3. Member States shall require that the information referred to in paragraph 1 can be accessed in a timely manner by competent authorities and FIUs.

4. Member States shall require that the information referred to in paragraph 1 is held in a central register when the trust generates tax consequences. The central register shall ensure timely and unrestricted access by competent authorities and FIUs, without alerting the parties to the trust concerned. It may also allow timely access by obliged entities, within the framework of customer due diligence in accordance with Chapter II. Member States shall notify to the Commission the characteristics of those national mechanisms.

5. Member States shall require that the information held in the central register referred to in paragraph 4 is adequate, accurate and up-to-date.

6. Member States shall ensure that obliged entities do not rely exclusively on the central register referred to in paragraph 4 to fulfil their customer due diligence requirements as laid down in Chapter II. Those requirements shall be fulfilled by using a risk-based approach.

7. Member States shall ensure that competent authorities and FIUs are able to provide the information referred to in paragraphs 1 and 4 to the competent authorities and to the FIUs of other Member States in a timely manner.

8. Member States shall ensure that the measures provided for in this Article apply to other types of legal arrangements having a structure or functions similar to trusts.

9. By 26 June 2019, the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring safe and efficient interconnection of the central registers. Where appropriate, that report shall be accompanied by a legislative proposal.

CHAPTER IV

REPORTING OBLIGATIONS

SECTION 1

General provisions

Article 32

1. Each Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing.

2. Member States shall notify the Commission in writing of the name and address of their respective FIUs.

3. Each FIU shall be operationally independent and autonomous, which means that the FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information. 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 the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing. It shall be able to obtain additional information from obliged entities.

Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks.

4. Member States shall ensure that their FIUs have access, directly or indirectly, in a timely manner, to the financial, administrative and law enforcement information that they require to fulfil their tasks properly. FIUs shall be able to respond to requests for information by competent authorities in their respective Member States when such requests for information are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing. The decision on conducting the analysis or dissemination of information shall remain with the FIU.

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

6. 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 the basis of that information.

7. Member States shall ensure that the FIU is empowered to take urgent action, directly or indirectly, where there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction that is proceeding, in order to analyse the transaction, confirm the suspicion and disseminate the results of the analysis to the competent authorities. The FIU shall be empowered to take such action, directly or indirectly, 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.

8. The FIU's analysis function shall consist of the following:

(a) an operational analysis which focuses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use of the information after dissemination; and

(b) a strategic analysis addressing money laundering and terrorist financing trends and patterns.

Article 33

1. Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly:

(a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, 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; and

(b) providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.

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

2. The person appointed in accordance with point (a) of Article 8(4) shall transmit the information referred to in paragraph 1 of this Article to the FIU of the Member State in whose territory the obliged entity transmitting the information is established.

Article 34

1. By way of derogation from Article 33(1), Member States may, in the case of obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), designate an appropriate self-regulatory body of the profession concerned as the authority to receive the information referred to in Article 33(1).

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

2. Member States shall not apply the obligations laid down in Article 33(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such exemption relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 35

1. Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to proceeds of criminal activity or to terrorist financing until they have completed the necessary action in accordance with point (a) of the first subparagraph of Article 33(1) and have complied with any further specific instructions from the FIU or the competent authorities in accordance with the law of the relevant Member State.

2. Where refraining from carrying out transactions referred to in paragraph 1 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 36

1. Member States shall ensure that if, in the course of checks carried out on the obliged entities by the competent authorities referred to in Article 48, or in any other way, those authorities discover facts that could be related to money laundering or to terrorist financing, they shall promptly inform the 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 37

Disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity in accordance with Articles 33 and 34 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 in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether illegal activity actually occurred.

Article 38

Member States shall ensure that individuals, including employees and representatives of the obliged entity, who report suspicions of money laundering or terrorist financing internally or to the FIU, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

SECTION 2

Prohibition of disclosure

Article 39

1. Obliged 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 Article 33 or 34 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, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between the credit institutions and financial institutions or between those institutions and their branches and majority-owned subsidiaries located in third countries, provided that those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group, in accordance with Article 45, and that the group-wide policies and procedures comply with the requirements laid down in this Directive.

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between the obliged entities as referred to in point (3)(a) and (b) of Article 2(1), or entities 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 larger structure to which the person belongs and which shares common ownership, management or compliance control.

5. For obliged entities referred to in points (1), (2), (3)(a) and (b) of Article 2(1) in cases relating 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 obliged entities provided that they are from a Member State, or entities 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 point (3)(a) and (b) of Article 2(1) seek to dissuade a client from engaging in illegal activity, that shall not constitute disclosure within the meaning of paragraph 1 of this Article.

CHAPTER V

DATA PROTECTION, RECORD-RETENTION AND STATISTICAL DATA

Article 40

1. Member States shall require obliged entities to retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;

(b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction.

Upon expiry of the retention periods referred to in the first subparagraph, Member States shall ensure that obliged entities delete personal data, 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 after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years.

2. Where, on 25 June 2015, legal proceedings concerned with the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing are pending in a Member State, and an obliged entity holds information or documents relating to those pending proceedings, the obliged entity may retain that information or those documents, in accordance with national law, for a period of five years from 25 June 2015. Member States may, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, allow or require the retention of such information or documents for a further period of five years where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing.

Article 41

1. The processing of personal data under this Directive is subject to Directive 95/46/EC, as transposed into national law. Personal data that is processed pursuant to this Directive by the Commission or by the ESAs is subject to Regulation (EC) No 45/2001.

2. Personal data shall be processed by obliged entities on the basis of this Directive only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Directive for any other purposes, such as commercial purposes, shall be prohibited.

3. Obliged entities shall provide new clients with the information required pursuant to Article 10 of Directive 95/46/EC before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of obliged entities under this Directive to process personal data for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 of this Directive.

4. In applying the prohibition of disclosure laid down in Article 39(1), Member States shall adopt legislative measures restricting, in whole or in part, the data subject's right of access to personal data relating to him or her to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned to:

(a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or

(b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.

Article 42

Member States shall require that their obliged entities have systems in place that enable them to respond fully and speedily to enquiries from their FIU or from other authorities, in accordance with their national law, as to whether they are maintaining or have maintained, during a five-year period prior to that enquiry a business relationship with specified persons, and on the nature of that relationship, through secure channels and in a manner that ensures full confidentiality of the enquiries.

Article 43

The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Directive 95/46/EC.

Article 44

1. Member States shall, for the purposes of contributing to the preparation of 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. The statistics referred to in paragraph 1 shall include:

(a) data measuring the size and importance of the different sectors which fall within 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 AML/CFT regime, including the number of suspicious transaction reports made to the FIU, the follow-up given to those reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences, the types of predicate offences, where such information is available, and the value in euro of property that has been frozen, seized or confiscated;

(c) if available, data identifying the number and percentage of reports resulting in further investigation, together with the annual report to obliged entities detailing the usefulness and follow-up of the reports they presented;

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

3. Member States shall ensure that a consolidated review of their statistics is published.

4. Member States 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 45

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

2. Member States shall require that obliged entities that operate establishments in another Member State ensure that those establishments respect the national provisions of that other Member State transposing this Directive.

3. Member States shall ensure that where obliged entities have branches or majority-owned subsidiaries located in third countries where the minimum AML/CFT 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 law so allows.

4. The Member States and the ESAs shall inform each other of instances in which a third country's law does not permit the implementation of the policies and procedures required under paragraph 1. In such cases, coordinated action may be taken to pursue a solution.

5. Member States shall require that, where a third country's law does not permit the implementation of the policies and procedures required under paragraph 1, obliged entities ensure that branches and majority-owned subsidiaries in that third country apply additional measures to effectively handle the risk of money laundering or terrorist financing, and inform the competent authorities of their home Member State. If the additional measures are not sufficient, the competent authorities of the home Member State 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.

6. The ESAs shall develop draft regulatory technical standards specifying the type of additional measures referred to in paragraph 5 and the minimum action to be taken by credit institutions and financial institutions where a third country's law does not permit the implementation of the measures required under paragraphs 1 and 3.

The ESAs shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 26 December 2016.

7. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 6 of this Article in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

8. Member States shall ensure that the 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.

9. Member States may require electronic money issuers as defined in point (3) of Article 2 of Directive 2009/110/EC and payment service providers as defined in point (9) of Article 4 of Directive 2007/64/EC 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, compliance with AML/CFT rules and to facilitate supervision by competent authorities, including by providing competent authorities with documents and information on request.

10. The ESAs shall develop draft regulatory technical standards on the criteria for determining the circumstances in which the appointment of a central contact point pursuant to paragraph 9 is appropriate, and what the functions of the central contact points should be.

The ESAs shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 26 June 2017.

11. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 10 of this Article in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

Article 46

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.

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

Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.

2. Member States shall ensure that obliged entities have access to up-to-date information on the practices of money launderers and financers of terrorism and on indications leading to the recognition of suspicious transactions.

3. Member States shall ensure that, where practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided to obliged entities.

4. Member States shall require that, where applicable, obliged entities identify the member of the management board who is responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this Directive.

SECTION 2

Supervision

Article 47

1. Member States shall provide that currency exchange and cheque cashing offices and trust or company service providers 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 the entities referred to in paragraph 1, or are the beneficial owners of such entities, are fit and proper persons.

3. With respect to the obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), Member States shall ensure that competent authorities take the necessary measures to prevent criminals convicted in relevant areas or their associates from holding a management function in or being the beneficial owners of those obliged entities.

Article 48

1. Member States shall require the competent authorities to monitor effectively, and to take the measures necessary to ensure, compliance with this Directive.

2. Member States shall ensure that the competent authorities have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate financial, human and technical resources to perform their functions. Member States shall ensure that staff of those authorities maintain high professional standards, including standards of confidentiality and data protection, that they are of high integrity and are appropriately skilled.

3. In the case of credit institutions, 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 those establishments respect the national provisions of that Member State transposing this Directive. In the case of the establishments referred to in Article 45(9), such supervision may include the taking of appropriate and proportionate measures to address serious failings that require immediate remedies. Those measures shall be temporary and be terminated when the failings identified are addressed, including with the assistance of or in cooperation with the competent authorities of the home Member State of the obliged entity, in accordance with Article 45(2).

5. Member States shall ensure that the competent authorities of the Member State in which the obliged entity operates establishments shall cooperate with the competent authorities of the Member State in which the obliged entity has its head office, to ensure effective supervision of the requirements of this Directive.

6. Member States shall ensure that when applying a risk-based approach to supervision, the competent authorities:

(a) have a clear understanding of the risks of money laundering and terrorist financing present in their Member State;

(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 obliged entities, and on the risks of money laundering and terrorist financing in that Member State.

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 their management and operations.

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 internal policies, controls and procedures.

9. In the case of the obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), Member States may allow the functions referred to in paragraph 1 of this Article to be performed by self-regulatory bodies, provided that those self-regulatory bodies comply with paragraph 2 of this Article.

10. By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 on the characteristics of a risk-based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis. Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

SECTION 3

Cooperation

Subsection I

National cooperation

Article 49

Member States shall ensure that policy makers, the FIUs, supervisors and other competent authorities involved in AML/CFT have effective mechanisms to enable them to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing, including with a view to fulfilling their obligation under Article 7.

Subsection II

Cooperation with the ESAs

Article 50

The competent authorities shall provide the ESAs with all the information necessary to allow them to carry out their duties under this Directive.

Subsection III

Cooperation between FIUs and with the Commission

Article 51

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 meetings of the EU FIUs' Platform composed of representatives from Member States' FIUs, in order to facilitate cooperation among FIUs, exchange views and provide advice on implementation issues relevant for FIUs and reporting entities as well as on cooperation-related issues such as effective FIU cooperation, the identification of suspicious transactions with a cross-border dimension, the standardisation of reporting formats through the FIU.net or its successor, the joint analysis of cross-border cases, and the identification of trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

Article 52

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

Article 53

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 that may be 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 FIU.net or its successor.

When an FIU receives a report pursuant to point (a) of the first subparagraph of Article 33(1) 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 available powers which it would normally use domestically for receiving and analysing information when it replies to a request for information referred to in paragraph 1 from another FIU. The FIU to whom the request is made shall respond in a timely manner.

When an FIU seeks to obtain additional information from an obliged entity established in another Member State which operates on its territory, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is established. That FIU shall transfer requests and answers promptly.

3. An FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law. Those exceptions shall be specified in a way which prevents misuse of, and undue limitations on, the free exchange of information for analytical purposes.

Article 54

Information and documents received pursuant to Articles 52 and 53 shall be used for the accomplishment of the FIU's tasks as laid down in this Directive. When exchanging information and documents pursuant to Articles 52 and 53, 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 55

1. Member States shall ensure that the information exchanged pursuant to Articles 52 and 53 is used only for the purpose for which it was sought or provided and that any dissemination of that information 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 consent by the FIU providing the information.

2. Member States shall ensure that the requested FIU's prior consent to disseminate the information to competent authorities is granted promptly and to the largest extent possible. The requested FIU shall 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 56

1. Member States shall require their FIUs to use protected channels of communication between themselves and encourage the use of the FIU.net or its successor.

2. Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs cooperate in the application of state-of-the-art technologies in accordance with their national law. Those technologies shall allow FIUs to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds.

Article 57

Differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law.

SECTION 4

Sanctions

Article 58

1. Member States shall ensure that obliged entities can be held liable for breaches of national provisions transposing this Directive in accordance with this Article and Articles 59 to 61. Any resulting sanction or measure shall be effective, proportionate and dissuasive.

2. Without prejudice to the right of Member States to provide for and impose criminal sanctions, Member States shall lay down rules on administrative sanctions and measures and ensure that their competent authorities may impose such sanctions and measures with respect to breaches of the national provisions transposing this Directive, and shall ensure that they are applied.

Member States may decide not to lay down rules for administrative sanctions or measures for breaches which are subject to criminal sanctions in their national law. In that case, Member States 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, sanctions and measures can be applied 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 all the supervisory and investigatory powers that are necessary for the exercise of their functions.

5. Competent authorities shall exercise their powers to impose administrative 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 other authorities;

(d) by application to the competent judicial authorities.

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

Article 59

1. Member States shall ensure that this Article applies at least to breaches on the part of obliged entities that are serious, repeated, systematic, or a combination thereof, of the requirements laid down in:

(a) Articles 10 to 24 (customer due diligence);

(b) Articles 33, 34 and 35 (suspicious transaction reporting);

(c) Article 40 (record-keeping); and

(d) Articles 45 and 46 (internal controls).

2. Member States shall ensure that in the cases referred to in paragraph 1, the administrative sanctions and measures that can be applied include at least the following:

(a) a public statement which identifies the natural or legal person and the nature of the breach;

(b) an order requiring the natural or legal person to cease the conduct and to desist from 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, held responsible for the breach, from exercising managerial functions in obliged entities;

(e) maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least EUR 1 000 000.

3. Member States shall ensure that, by way of derogation from paragraph 2(e), where the obliged entity concerned is a credit institution or financial institution, the following sanctions can also be applied:

(a) in the case of a legal person, maximum administrative pecuniary sanctions of at least EUR 5 000 000 or 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 is required to prepare consolidated financial accounts in accordance with Article 22 of Directive 2013/34/EU, the relevant total annual turnover shall be the total annual turnover or the corresponding type of income in accordance with the relevant accounting Directives according to the last available consolidated accounts approved by the management body of the ultimate parent undertaking;

(b) in the case of a natural person, maximum administrative pecuniary sanctions of at least EUR 5 000 000, or in the Member States whose currency is not the euro, the corresponding value in the national currency on 25 June 2015.

4. Member States may empower competent authorities to impose additional types of administrative sanctions in addition to those referred to in points (a) to (d) of paragraph 2 or to impose administrative pecuniary sanctions exceeding the amounts referred to in point (e) of paragraph 2 and in paragraph 3.

Article 60

1. Member States shall ensure that a decision imposing an administrative sanction or measure for breach of the national provisions transposing this Directive against which there is no appeal shall be published by the competent authorities on their official website immediately after the 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 persons responsible. Member States shall not be obliged to apply this subparagraph to decisions imposing measures that are of an investigatory nature.

Where the publication of the identity of the persons responsible as referred to in the first subparagraph or the personal data of such 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 jeopardises the stability of financial markets or an on-going investigation, competent authorities shall:

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

(b) publish the decision to impose an administrative sanction or measure on an anonymous basis in a manner in accordance with national law, if such anonymous publication ensures an effective protection of the personal data concerned; in the case of a decision to publish an administrative 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 an administrative sanction or measure at all in the event that the options set out in points (a) and (b) 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 the decision with regard to measures which are deemed to be of a minor nature.

2. 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 an administrative sanction or a measure shall also be published.

3. 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. However, 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.

4. Member States shall ensure that when determining the type and level of administrative sanctions or measures, the competent authorities shall take into account all relevant circumstances, including where applicable:

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

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

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

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

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

(f) the level of cooperation of the natural or legal person held responsible with the competent authority;

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

5. Member States shall ensure that legal persons can be held liable for the breaches referred to in Article 59(1) committed for their benefit by any person, acting individually or as part of an organ of that legal person, and having a leading position within the legal person based on any of the following:

(a) power to represent the legal person;

(b) authority to take decisions on behalf of the legal person; or

(c) authority to exercise control within the legal person.

6. 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 5 of this Article has made it possible to commit one of the breaches referred to in Article 59(1) for the benefit of that legal person by a person under its authority.

Article 61

1. Member States shall ensure that competent authorities establish effective and reliable mechanisms to encourage the reporting to competent authorities of potential or actual breaches of the national provisions transposing this Directive.

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) appropriate protection for the accused person;

(d) protection of personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach, in compliance with the principles laid down in Directive 95/46/EC;

(e) 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 62

1. Member States shall ensure that their competent authorities inform the ESAs of all administrative sanctions and measures imposed in accordance with Articles 58 and 59 on credit institutions and financial institutions, including of any appeal in relation thereto and the outcome thereof.

2. Member States shall ensure that their competent authorities, in accordance with their national law, check the existence of a relevant conviction in the criminal record of the person concerned. Any exchange of information for those purposes shall be carried out in accordance with Decision 2009/316/JHA and Framework Decision 2009/315/JHA as implemented in national law.

3. The ESAs shall maintain a website with links to each competent authority's publication of administrative sanctions and measures imposed in accordance with Article 60 on credit institutions and financial institutions, and shall show the time period for which each Member State publishes administrative sanctions and measures.

CHAPTER VII

FINAL PROVISIONS

Article 63

Point (d) of paragraph 2 of Article 25 of Regulation (EU) No 648/2012 of the European Parliament and the Council ([1]) is replaced by the following:

'(d) the CCP is established or authorised in a third country that is not considered, by the Commission in accordance with Directive (EU) 2015/849 of the European Parliament and of the Council (*), as having strategic deficiencies in its national anti-money laundering and counter financing of terrorism regime that poses significant threats to the financial system of the Union.

(*) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).'.

Article 64

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 9 shall be conferred on the Commission for an indeterminate period of time from 25 June 2015.

3. The power to adopt delegated acts referred to in Article 9 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect on the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 9 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of one month of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by one month at the initiative of the European Parliament or of the Council.

Article 65

By 26 June 2019, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and to the Council.

Article 66

Directives 2005/60/EC and 2006/70/EC are repealed with effect from 26 June 2017.

References to the repealed Directives shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex IV.

Article 67

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 26 June 2017. They shall immediately communicate the text of those measures to the Commission.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

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.

([1]) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

Article 68

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

Article 69

This Directive is addressed to the Member States.

Done at Strasbourg, 20 May 2015.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	Z. KALNIŅA-LUKAŠEVICA

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 13(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 16:

(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 that are resident in geographical areas of lower risk as set out in point (3);

(2) Product, service, transaction or delivery channel risk factors:

(a) life insurance policies for which the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

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

(3) Geographical risk factors:

(a) Member States;

(b) third countries having effective 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, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers that are resident in geographical areas of higher risk as set out in point (3);

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) businesses that are cash-intensive;

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

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

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

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(3) Geographical risk factors:

(a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

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

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

This Directive	Directive 2005/60/EC	Directive 2006/70/EC
—		Article 1
—		Article 3
—		Article 5
—		Article 6
—		Article 7
Article 1	Article 1	
Article 2	Article 2	
Article 2(3) to (9)		Article 4
Article 3	Article 3	
Article 3(9), (10) and (11)		Article 2(1), (2) and (3)
Article 4	Article 4	
Article 5	Article 5	
Articles 6 to 8	—	
Article 10	Article 6	
Article 11	Article 7	
Article 13	Article 8	
Article 14	Article 9	
Article 11(d)	Article 10(1)	
—	Article 10(2)	
Articles 15, 16 and 17	Article 11	
—	Article 12	
Articles 18 to 24	Article 13	
Article 22		Article 2(4)
Article 25	Article 14	
—	Article 15	
Article 26	Article 16	
—	Article 17	
Article 27	Article 18	
Article 28	—	
Article 29	Article 19	
Article 30	—	
Article 31	—	
—	Article 20	
Article 32	Article 21	
Article 33	Article 22	

This Directive	Directive 2005/60/EC	Directive 2006/70/EC
Article 34	Article 23	
Article 35	Article 24	
Article 36	Article 25	
Article 37	Article 26	
Article 38	Article 27	
Article 39	Article 28	
—	Article 29	
Article 40	Article 30	
Article 45	Article 31	
Article 42	Article 32	
Article 44	Article 33	
Article 45	Article 34	
Article 46	Article 35	
Article 47	Article 36	
Article 48	Article 37	
Article 49	—	
Article 50	Article 37a	
Article 51	Article 38	
Articles 52 to 57	—	
Articles 58 to 61	Article 39	
—	Article 40	
—	Article 41	
—	Article 41a	
—	Article 41b	
Article 65	Article 42	
—	Article 43	
Article 66	Article 44	
Article 67	Article 45	
Article 68	Article 46	
Article 69	Article 47	