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)

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. Directive 2001/97/EC of the European Parliament and of the Council[(5)] 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[(6)] and in Commission Directive 2006/70/EC[(7)].

(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[(8)], 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.

(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[(9)], 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[(10)], and the European Supervisory Authority (European Securities and Markets Authority) (ESMA), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council[(11)], 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.

(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[(12)], 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[(13)] 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[(14)], 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 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[(15)] 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 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[(16)] and Council Decision 2009/316/JHA[(17)], 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[(18)], 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[(19)],

HAVE ADOPTED THIS DIRECTIVE:

(**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).

(**5**) 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).

(**6**) 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).

(**7**) 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).

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

(**9**) 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).

(**10**) 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).

(**11**) 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).

(**12**) 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).

(**13**) 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).

(**14**) 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).

(**15**) 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).

(**16**) 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).

(**17**) 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).

(**18**) OJ C 369, 17.12.2011, p. 14.

(**19**) OJ C 32, 4.2.2014, p. 9.