Opinion of the European Data Protection Supervisor

on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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[1],

Having regard to 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[2], and in particular Article 28(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 5 February 2013, the Commission adopted two proposals: one for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[3] ("the proposed Directive"), and one for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds[4] ("the proposed Regulation"), hereinafter jointly referred to as "the Proposals". The Proposals were sent to the EDPS for consultation on 12 February 2013.

2. The EDPS welcomes the fact that he is consulted by the Commission and that a reference to the consultation is included in the preambles of the Proposals.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM (2013) 45 final.
[4] COM (2013) 44 final.

3. Before the adoption of the Proposals, the EDPS was given the possibility to provide informal comments to the Commission. Some of these comments have been taken into account.

1.2. Objectives and scope of the Proposals

4. Money laundering means, broadly speaking the conversion of the proceeds of criminal activity into apparently clean funds, usually *via* the financial system[5]. This is done by disguising the sources of the money, changing its form, or moving the funds to a place where they are less likely to attract attention. Terrorist financing is the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used in order to carry out terrorist offences[6].

5. At EU level, legislation has been introduced with the aim to prevent money laundering and terrorist financing as from 1991. These offenses are considered as a threat to the integrity and stability of the financial sector and, more in general, as a threat to the Internal Market. The legal basis for the Proposals is Article 114 of TFEU.

6. The EU rules designed to prevent money laundering are to a large extent based on standards adopted by the Financial Action Task Force (FATF)[7]. The Proposals aim at implementing in the EU the revised anti money laundering international standards introduced by the FATF in February 2012. The current directive, the so-called Third Anti-Money Laundering (AML) Directive[8], is in force since 2005. It provides a European framework around the international FATF standards.

7. The Third AML Directive applies to the financial sector (credit institutions, financial institutions) as well as to professionals such as lawyers, notaries, accountants, real estate agents, casinos and company service providers. Its scope also encompasses all providers of goods, when payments are made in cash in excess of EUR 15.000. All these addressees are considered "obliged entities". The Directive requires these obliged entities to identify and verify the identity of customers (so-called customer due diligence, hereinafter 'CDD') and beneficial owners, and to monitor the financial transactions of the customers. It then includes obligations to report suspicions of money laundering or terrorist financing to the relevant Financial Intelligence Units (FIUs), as well as other accompanying obligations. The Directive also introduces additional requirements and safeguards (such as the requirement to conduct enhanced customer due diligence) for situations of higher risk.

---

[5] See Article 1(2) of the proposed Directive.

[6] See Article 1(4) of the proposed Directive.

[7] FATF is the global standard-setter for measures to combat money-laundering, terrorist financing, and (most recently) the financing of proliferation. It is an intergovernmental body with 36 members, and with the participation of over 180 countries. The European Commission is one of the founding members of the FATF. 15 EU Member States are FATF members in their own right.

[8] Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

8. The proposed Directive extends the scope of the current framework and aims at strengthening these obligations, for instance by including providers of gambling services and dealers in goods in the obliged entities, with a threshold of EUR 7500, requires extended beneficial ownership information, tightens the requirements on "politically exposed persons" and introduces requirements for scrutiny of family and close associates of all politically exposed persons. The list of predicate[9] offences for money laundering has been expanded to include tax crimes related to direct taxes and indirect taxes.

9. The proposed Regulation replaces Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds (hereinafter also referred to as the "Funds Transfers Regulation") which has the aim to improve traceability of payments. The Funds Transfers Regulation complements the other AML measures by ensuring that basic information on the payer of transfers of funds is immediately available to law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists.

2. GENERAL ANALYSIS OF THE PROPOSALS

2.1. Introductory remarks

Necessity to take account of data protection requirements

10. The EDPS understands the need to implement the new set of Recommendations issued by the FATF in February 2012[10] in the European anti money laundering framework. He recognises the importance of anti money laundering policies for economical and financial reputation of Member States, and more in general as an instrument in the combat of serious crimes. He however wishes to highlight that European data protection standards have no equivalent at the international level of the FATF and that the search for consistency in anti-money laundering policies at international level should not result in ignoring EU data protection requirements. The EDPS recalls that the right of an individual to the protection of his or her personal data is safeguarded in Article 16 TFEU and in Article 8 of the Charter of the Fundamental Rights of the Union.

11. Achieving transparency of payments sources, funds deposits and transfers in order to counter terrorism and money laundering is a legitimate interest, but it needs to be pursued while ensuring compliance with data protection requirements. The EDPS therefore insists on the necessity to take these requirements into account while transposing the FAFT standards in the EU legal order.

12. The EDPS also wishes to draw the attention of the legislators on the fact that the proposed Directive and Regulation both impact on the relationships between the service provider and the customer, and that the collection of data for anti money laundering purposes takes place at the same time as the collection of data for

[9] A predicate offence is any criminal offence whose proceeds are used to commit another offence: in this context, for instance, criminal activity predicate to money laundering can be fraud, corruption, drug dealing and other serious crimes.
[10] See in particular Recommendation 16.

commercial purposes. For instance, data will be collected for CDD purposes by the obliged entity at the same time as data necessary to establish the business relationship (see Article 10 of the proposed Directive), for verification purposes, when a transfer of funds is sent or received by a payment service provider established in the Union (see Article 3 of the Proposed Regulation). Sometimes, the same data (such as the identity of the customer) will be collected at the same time for both commercial and anti-money laundering purposes.

13. One of the concerns of the EDPS is that the customer is not properly informed, at the moment of collection, for which purpose the data is required and processed. This right to be informed is laid down in Directive 95/46/EC and is needed to give effect to the rights of access and rectification that are included in Article 8 of the Charter.

14. The EDPS also notes that the proposals will result in increasing amounts of data being collected for anti money laundering and anti terrorist purposes, which will increase the possible consequences for data subjects. In particular, the proposed Directive involves the scrutiny of financial transactions of customers of financial and credit institutions, as well as customers of a number of other categories of service providers whose activities are related to economic activities. This involves an intense processing of customers' personal data which can lead ultimately to investigations by law enforcement authorities. *Per se*, the proposed Directive has an important impact on the individuals' right to protection of their personal data. The proposed Regulation sets an obligation to collect personal data on the payer and the beneficiary of funds and sometimes involves the transfer of these data to organisations or branches established in third countries.

15. The EDPS therefore insists on the necessity to ensure that data protection safeguards are concretely applied to this specific area and developed in the text so that the customer's awareness is raised and that he/she benefits from legal certainty and from the full protection provided by the EU data protection legislation. These safeguards, as described below, will also ensure that the customer is not subject to decisions based upon data that should not have been collected, that have been unduly stored or that are not or no longer accurate. In this context, attention is drawn to Article 8(2) of the Charter which grants everyone the right to have data concerning him or her rectified.

16. The customer will not be the only one benefiting from data protection safeguards. Professionals responsible for carrying out the CDD laid down in the proposed Directive or the data collection and verification necessary to a transfer of funds will also enjoy adequate protection against the arbitrary publication of sanctions and of their data in case they are considered not to have fulfilled their obligations. Data protection should not be perceived as an obstacle to anti money laundering obligations but as a basic requirement necessary to achieve this purpose while respecting the fundamental right to the protection of one's personal data.

17. The EDPS underlines that neither the proposed Directive nor the Regulation clarify the application of EU data protection rules to the specific processing activities involved and that no substantial provision addresses data protection

issues. In this Opinion, he asks for introduction of safeguards that should apply anytime personal data is processed.

18. Finally, the EDPS notes that data protection was raised as a concern in the Study on the application of the Regulation on information accompanying transfers of funds[11] carried out by the Commission. The Study also recommends clarifying data protection requirements when extending the scope of the Fund Transfers Regulation. The Impact Assessment for the proposed Directive highlights in several instances the difficulties that private stakeholders encounter as regards 'their ability to comply with AML requirements while at the same time adhering to rules aimed at ensuring a high level of protection of personal data'. The identified difficulties include sharing of information within the group of undertakings, consent of the data subject, record keeping and legal uncertainties with regard to processing of AML/CTF[12] related data within entities. Also sharing of information between FIUs is perceived as problematic.

2.2. Consequences

Reference to applicable data protection law

19. The EDPS insists on the fact that it is essential to explicitly mention the applicable EU data protection law in a substantive provision of the Proposals: a mere reference to general principles in recitals[13] cannot be considered as sufficient. Such a substantive provision is needed from the point of view of legal certainty, to avoid any ambiguity on the fact that the Proposals should not be considered as derogations from the data protection framework which remains fully applicable to the envisaged processing operations. The EDPS therefore recommends stating explicitly that the Proposals are without prejudice to the applicable data protection laws. For the sake of clarity, he further recommends that the references to the applicable data protection legislation are grouped in a single provision of the proposed Directive, as well as in a single provision of the proposed Regulation.

20. Reference should be made to the national laws implementing Directive 95/46/EC. Moreover, a reference to the applicability of Regulation (EC) No 45/2001 should also be included due to the involvement of European supervisory authorities.

21. A good example of a substantive provision can be found in Article 22 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation[14], which explicitly provides as a general rule that (national rules implementing) Directive 95/46/EC (and Regulation (EC) No 45/2001) applies to the processing of personal data within the framework of the proposal.

[11] European Commission DG Internal Market and Services (DG MARKT), Study on the application of the Regulation on information accompanying transfers of funds, MARKT/2011/054/F.
[12] Combating Terrorism Financing.
[13] Currently recitals 30 and 34 in the proposed Directive and recital 7 of the proposed Regulation.
[14] Commission proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, COM(2011) 651. The text is undergoing review by the European Parliament and the Council according to the ordinary legislative procedure.

22. The EDPS recalls that recital 33 of the proposed Directive refers to 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[15]. This Framework Decision applies -subject to a number of exceptions- to the processing for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

23. The EDPS notes that the Proposals are based on Article 114 TFEU (internal market), and not on Article 87 TFEU (police cooperation). This choice of a legal basis implies that the activities planned under the Proposals do not include activities of competent authorities in the Member States in the meaning of Article 87 TFEU, which includes police, customs and other specialised law enforcement services dealing with the prevention, detection and investigation of criminal offences.

24. As a consequence of this choice of a legal basis, the Council Framework Decision would not be applicable in the context of the Proposals. Instead, the processing operations of personal data as regards money laundering would include the activities of service providers in the internal market[16] and not "operations concerning public security and the activities of the State in areas of criminal law".[17] As a result, all processing operations would fall under Directive 95/46/EC and Regulation (EC) No 45/2001, and the reference to the Council Framework Decision in the recital would no longer be needed and should be deleted. The EDPS would welcome consistency in that regard.

25. However, this result can only be reached if the "competent authorities" and "FIUs" referred to in the proposed directive do not qualify as authorities within the meaning of Article 87 TFEU, and in any event that their activities do not fall under the scope of police cooperation. Only in this scenario would Directive 95/46/EC and Regulation (EC) No 45/2001 be fully applicable. The comments on competent authorities and FIUs (see points 29-32) must be seen in this context.

Other consequences

26. The EDPS recalls that clarifying the applicable data protection legislation is essential but not sufficient. The references to applicable data protection law should be specified in concrete safeguards that will apply to any situation in which personal data processing is envisaged (see on this point 62 and following).

27. Moreover, any specifications of data protection principles to be set forth in the context of anti money laundering have to be justified. For instance, the chosen data retention period should correspond to a demonstrated necessity of keeping the data for a certain amount of time. Likewise, the restriction of data subjects' rights should only take place by way of an exception on the basis of a well-described and

[15] OJ L 350, 30.12.2008, p. 60.
[16] Judgment of the Court of 10 February 2009, Ireland v. European Parliament and Council of the European Union (C-301/06), ECR , p. I-00593, para 91.
[17] Judgment of the Court of 30 May 2006, European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), ECR p. I-04721.

explained necessity and provided that such a restriction is strictly limited in view of the justifications given. Furthermore, the proportionality of the systematic publication of administrative sanctions is not assessed.

28. Besides, the EDPS wishes to highlight the need to respect the principle of proportionality, which means in the present context that there is a need to strike the appropriate balance between two different interests, namely the fight against money laundering and the protection of one's personal data.

2.3. Common general comments

2.3.1. "Competent authorities" and "FIUs"

29. The proposed Directive provides for the exchange of information, and possibly of personal data, between FIUs established in the various Member States, between competent authorities and EBA, EIOPA and ESMA[18], and between FIUs and the Commission (see Articles 46 to 53).

30. The concept of "competent authorities" is not defined in the proposed Directive or in the Third AML Directive, and definitions in the First and Second AML Directive do not specify the nature of these authorities. The First AML Directive (91/308/EEC)[19]defines competent authorities as follows: "Competent authorities means the national authorities empowered by law or regulation to supervise credit or financial institutions". In the Second AML Directive (2001/97/EC)[20], the concept of "Competent authorities" means the "national authorities empowered by law or regulation to supervise the activity of any of the institutions or persons subject to this Directive".

31. The nature of FIUs also requires clarifications. Article 31 of the proposed Directive states that the FIU is supposed to be a central national unit responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, information which concerns potential money laundering or associated predicate offences, potential terrorist financing or is required by national legislation or regulation. Article 49 does not clarify their nature either, as it states that FIUs are "law enforcement or judicial or hybrid authorities". As a matter of fact, the nature of FIUs can vary across Member States, from branches of quasi-police bodies to departments of entities charged with purely financial supervisory roles[21].

---

[18] European Banking Authority ("EBA"), European Insurance and Occupational Pensions Authority (hereinafter "EIOPA") and European Securities and Markets Authority (hereinafter "ESMA").

[19] 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 , 28.06.1991, p.77-83.

[20] 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. 76–82.

[21] The list of members of the Egmont Group -an informal group of FIUs established in 1995- includes, for instance, a department of the Bank of Italy, the UKFIU within the Serious Organised Crime Agency-SOCA; the TRACFIN within the French Ministry of Economy and finances. See www.egmontgroup.org.

32. In order to ensure seamless and effective data protection, and in view of the legal basis chosen for the Proposals[22], there should be no doubt that the activities of the competent authorities and the FIUs under the proposed Directive will only be subject to national provisions implementing Directive 95/46/EC. The EDPS therefore recommends adding a definition of "competent authorities" and "FIUs" in the proposed Directive to clarify, at the very least, that "competent authorities" in the context of the proposed Directive are not to be considered as "competent authorities" within the meaning of Article 2(h) of the Framework Decision 2008/977/JHA[23]. Despite the fact that they may have tasks similar to those of law enforcement authorities, they should -in the activities covered by the proposed Directive- not be considered as police or judicial authorities.

2.3.2. Legal basis for processing and purpose limitation principle

Legitimate grounds for processing

33. The EDPS notes that recital 32 of the proposed Directive mentions that the fight against money-laundering and terrorist financing is recognised as an important public interest ground by all Member States. However, this recognition has no relevance for the legitimate ground for data processing referred to in Article 7(e) of Directive 95/46/EC. In the context of the proposed Directive, the relevant legitimate ground for the processing of personal data should more appropriately be the necessity to comply with a legal obligation by the obliged entities, competent authorities and FIUs (i.e. Article 7(c) of Directive 95/46/EC). The EDPS proposes specifying this in the recital, for reasons of legal certainty.

Purpose limitation principle

34. The EDPS welcomes that recital 31 of the proposed Directive aims at complying with the purpose limitation principle, since it states that the sole purpose of the processing must be the prevention of money laundering and terrorist financing. Data must not be further processed for incompatible purposes. The EDPS recalls that Directive 95/46/EC prohibits further processing of personal data collected for a specified, explicit and legitimate purpose in a way incompatible with that purpose (Article 6(1)(b)). The recently adopted Opinion of the Article 29 Working Party on purpose limitation[24] clarifies the criteria on the basis of which an evaluation of compatibility of purpose should be carried out. In particular, factors such as the impact on the individual of the further processing and concrete possible negative consequences are considered signs of likely incompatible use.

22 See points 27-30 above.

[23] 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. 6071.

[24] Article 29 Working Party Opinion 3/2013 on purpose limitation adopted on 3 April 2013, p. 26, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

On the prohibition of the processing of data collected for AML purposes for commercial purposes

35. Recital 31 of the proposed Directive and recital 7 of the proposed Regulation state that the processing of personal data for commercial purposes is prohibited.[25] The EDPS underlines that a risk of "function creep" exists, which may lead to the further use of data initially collected for anti money laundering and anti terrorist purposes for commercial/marketing purposes. For these reasons, the reference in a recital cannot be considered as sufficient. In this context, the EDPS recommends that the specific prohibition to process data for commercial purposes is inserted in a substantive provision of the proposed Directive and of the proposed Regulation.

The possible inclusion of tax crimes in the list of criminal activities tackled under the proposed Directive

36. The EDPS takes note of the proposed extension of the list of "criminal activities" that can be considered predicate offences for money laundering (Article 3(2)(4)(f) of the proposed Directive) to also include tax crimes. This is relevant in relation to the requirement for obliged entities to report to the relevant FIU where they know, suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity (Article 32). According to the Explanatory Memorandum[26], using the proceeds of an activity that qualifies as tax crime pursuant to the definition of Article 3(2)(4)(f) should also be considered as money laundering. As a consequence, obliged entities will have to promptly inform the FIU.

37. However, the EDPS notes a clear discrepancy with further statements in the explanatory memorandum, according to which "[T]he enhancement of the customer due diligence procedures for AML purposes *will also assist the fight against tax fraud and tax evasion*."[27] The proposed Directive refers to the Commission Communication related to the fight against tax fraud and evasion[28] which states that the enhancement of customer due diligence and increased transparency on beneficial owners could also "facilitate the use of relevant data for taxation purposes, e.g. to improve the effectiveness of the treatment of offshore investment structures under the EU Savings Taxation Directive".

38. The EDPS takes the view that such references in the Explanatory Memorandum do not and should not have the effect of including the fight against tax evasion among the purposes of data processing under the Proposals. This follows from the generally applicable purpose limitation principle enshrined in Directive 95/46/EC and explained above. Consequently, the legal effect of the insertion of tax crimes in the list of predicate offences would be to extend the information obligation to cases where obliged entities know or suspect that a tax crime is at the origin of a

[25] See on this: Study on the application of the Regulation on information accompanying transfers of funds, MARKT/2011/054/F, p. 97: "any comprehensive reporting of beneficiary information may violate data protection and privacy rights of customers and could be abused for commercial reasons by those payment service providers ("PSPs") who receive such information (who may use this information to directly contact their competitors' customers".
[26] Explanatory Memorandum p. 5
[27] Explanatory Memorandum, p. 5.
[28] Commission Communication presenting an Action Plan to strengthen the fight against tax fraud and evasion, adopted by the Commission on 6 December 2012, COM(2012)722 final, p. 10.

transfer of funds, while the overall objectives of the Proposals, i.e. the fight against money laundering and terrorist financing would remain unchanged. To avoid any doubt and in the interest of legal certainty, the EDPS recommends clarifying this aspect in a dedicated recital.

2.3.3. Exchange of data with third countries

39. Both the proposed Directive and the proposed Regulation involve significant exchanges of personal data with third countries which do not necessarily offer an adequate level of protection of personal data.

40. The rules on transfer of personal data to third countries are laid down in Articles 25 and 26 of Directive 95/46/EC. They prohibit the transfer of personal data when the level of protection in the country of the recipient is not adequate and set up strict conditions to the use of exceptions. Pursuant to Article 26(1) of Directive 95/46/EC, there are limited grounds on the basis of which transfer of personal data to third countries may take place by way of derogation to the "adequacy" principle of Article 25.

41. Moreover, the Article 29 Working Party Opinion on the interpretation of Article 26 of Directive 95/46/EC[29] states that a multinational company should not make 'significant transfers of data to a third country without providing an appropriate framework for the transfer, when it has the practical means of providing such protection (e.g. a contract, BCR, a convention).'[30] The WP29 then recommends that transfers of personal data, which might be qualified as repeated, mass or structural should, where possible, in view of their importance, only be carried out if adequate safeguards are adduced, which could be contracts or binding corporate rules.

Transfers under the proposed Directive

42. In the context of the proposed Directive, international transfers of personal data may take place in relation to obliged entities with branches or majority owned subsidiaries in countries outside the EU (according to Article 42(2)). These entities may need, for instance, to transfer CDD data among their branches and subsidiaries in order to be able to share information about certain customers' activities.

Transfers under the proposed Regulation

43. Any transfer of funds amounting to more than 1.000 EUR where the PSP of the payee is established outside the Union will result in the simultaneous transfer, by the PSP of the payer, of the name of the payer, the payer's account number, the payer's address or national identity number, or customer identification number or

[29] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 25 November 2005 2093/05/EN, WP 114, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf .
[30] Ibidem, page 9.

date and place of birth, the name of the payee and the payee's account number[31]. This transfer of personal data can be qualified as repeated (taking place every time a transfer of funds respecting the above-mentioned conditions takes place), massive (the amount of data potentially collected is quite large) and structural (the transfer of data is set as a common rule and could not be qualified as an exception). Moreover, more data will be collected and transferred on the payer and the payee when the transfer of funds takes place from the Union to countries outside the Union (complete information) than when it is made within the Union (simplified information)[32].

Consequences

44. Considering the repeated, mass and structural transfer of personal data that will take place in the framework of the proposed Directive and Regulation, the EDPS recommends including dedicated substantive provisions on the transfer of personal data to ensure proper protection of data subjects when data are transferred.

45. Unfortunately, Article 42 of the proposed Directive is very vague in relation to data transfers and in any case leaves a broad margin of discretion to obliged entities which could always claim that the application of data protection requirements in the third country would not be compatible with the local legislation.

46. The issue of mass transfer of personal data to third countries that do not ensure an adequate level of data protection is only addressed in recital 32 of the proposed Directive, which underlines that the fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States. Similarly, recital 7 of the proposed Regulation underlines that the transfer of personal data is necessary for an important public interest ground. Both Proposals therefore suggest that as these transfers pursue an important public interest ground, they would fall within the scope of the derogation set forth in Article 26(1)(d) of Directive 95/46/EC and would therefore respect data protection law.

47. The EDPS is of the opinion that one can not justify the use of the derogation set forth in Article 26(1)(d) by a statement that the transfer will take place under an important public interest ground. Transfers under a recognized important public interest ground can only be allowed after a careful assessment on a case by case basis[33]. He therefore recommends inserting a substantive provision in the

[31] Article 4 lists the information on the payer and the payee that should accompany a transfer of funds. Article 5 limits the number of data transferred when the PSPs of both payer and payee are established within the Union but, *a contrario* implies that a comprehensive set of data, as listed in Article 4, will have to be sent if the PSP of the payee is established outside the Union, with the exceptions described in Article 6.

[32] This is reflected in recitals 11 and 12. [32] See also Fund transfer proposed Regulation, p. 88. "[...] when sending funds to countries where there is no or little safeguard against the receiving institution (ab)using the information or indeed passing it on to third parties, the risk for the concerned individual could be significant. Since approximately 85% of the transactions processed by MVTS A are directed at countries outside the EU, including countries with weak legal systems, this is a real concern to this business".

[33] As already stated by the EDPS in the Opinion of 7 March 2012 on the data protection reform package, pt 225-227.

proposed Directive as well as in the proposed Regulation to provide for an appropriate legal basis for the intra-group/PSP to PSP transfers which would respect the text and the interpretation of Article 26 of Directive 95/46/EC.

2.3.4. Publication of administrative sanctions

48. Article 56(2)(a) of the proposed Directive and Article 18(2)(a) of the proposed Regulation provide that Member States should include in the list of sanctions related to certain violations[34] at least 'a public statement which indicates the natural or legal person and the nature of the breach'.

49. Both texts also provide for the automatic publication of a sanction or measure imposed for any breach without undue delay, including information on the identity of persons responsible for it (Articles 57 of the proposed Directive and 19 of the Proposed Regulation). Publication can be avoided if it would 'seriously jeopardize the stability of financial markets'. Also, when publication would cause a 'disproportionate damage to the parties involved', sanctions should be published on an anonymous basis. Such obligation will apply to natural persons but the categories of data to be collected and published are not specified.

50. As the EDPS highlighted on several occasions[35], the mandatory and automatic publication of sanctions, as it is currently formulated, does not meet the requirements of data protection law as clarified by the Court of Justice in the *Schecke* judgment. It should be borne in mind that, in order to assess the compliance with data protection requirements of a provision requiring public disclosure of personal information, it is of crucial importance to have a clear and well-defined purpose which the envisaged publication intends to serve. Only with a clear and well-defined purpose can it be assessed whether the publication of personal data involved is actually necessary and proportionate. In this context it is not sufficient that Article 17(1) contains the usual provision that Member States "lay down sanctions that are effective, proportionate and dissuasive". The Court of Justice underlined that the institutions should explore different methods to find the one which would be consistent with the objective of publication, while causing the least interference with the subjects´ right to private life and to protection of personal data.

51. The EDPS considers that the purpose, necessity and proportionality of an automatic publication of the sanctions are not assessed in an appropriate manner. In any event, adequate safeguards against the risks for the rights of the individuals should have been laid down. The EDPS notes in this context that, although in most Member States sanctions can be published, the publication is never

[34] Related to CDD rules, suspicious transaction reporting, record keeping and internal controls.

[35] See for instance, EDPS Opinion on the Commission proposals for a Directive of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council, and for a Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation on OTC derivatives, central counterparties and trade repositories, available on EDPS website at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-02-10_Financial_instruments_EN.pdf.

automatic[36]. Moreover, the Impact Assessment does not indicate whether less intrusive methods than the obligation to publish any sanction or measure might have guaranteed the same result in terms of the objective pursued while at the same time causing less interference with the privacy rights of the individuals concerned.

52. In addition, since under Article 56(2)(a) of the proposed Directive the competent authorities already have, among their sanctioning powers, the power to issue a public statement indicating the person responsible and the nature of the breach, it is not clear how the publication obligation under Article 57 relates to the power to issue a public statement under Article 56(2)(a).

53. The possibility to assess the necessity of publication on a case by case basis in light of the specific circumstances (for instance, the seriousness and type of breach) would constitute a more proportionate approach and would therefore be a preferred option compared to the mandatory and automatic publication in all cases. The text of the proposed Directive should therefore be modified in this sense.

54. Furthermore, safeguards are necessary in relation to the right of the accused persons to challenge a decision before the competent authority and their right to the presumption of innocence. The text of the Directive should specify that competent authorities are obliged to take appropriate measures to preserve both rights where the decision is subject to an appeal and where it is eventually annulled by a competent authority.

55. In addition, if the publication takes place on the Internet, it raises the specific issue of how to ensure that the information is kept online for no longer than is necessary and that the data cannot be manipulated or altered. Furthermore, the use of external search engines entails the risk that the information could be taken out of context and channelled through and outside the web in ways which cannot be easily controlled.

56. In view of these considerations, the EDPS, recommends evaluating alternative and less intrusive options to the general publication obligation and, in any case, specifying in the proposed Directive:
    - the purpose of such a publication if it was to be maintained;
    - the personal data that should be published;
    - that data subjects are to be informed before the publication of the decision and are guaranteed rights to appeal this decision before the publication is carried out;
    - that data subjects have the right to object under Article 14 of Directive 95/46/EC on compelling legitimate grounds.

57. The proposed Directive and the proposed Regulation should also provide that the authorities responsible for the publication must ensure that the personal data of the

[36] Impact Assessment, pages 92-93 and Annex VIII, pages 123 and following. Page 128 also mentions that almost all public sector stakeholders reported that the available sanctions are sufficient and proportionate to the severity of the breach.

persons concerned are kept online only for a reasonable period of time, after which they should be systematically deleted. They should also guarantee that these data are updated on a regular basis. Moreover, these authorities should be required to ensure that adequate security measures and safeguards are put in place, especially to protect data subjects from the risks related to the use of external search engines.

2.3.5. Data retention

58. The manner in which the issue of data retention periods is addressed in the proposed Directive and the proposed Regulation raises concerns.

59. Under Directive 95/46/EC, data exchanged should only be kept for the time necessary to achieve the purposes for which they were collected[37] and should be automatically deleted following the expiry of the retention period. This period of time should be justified and motivated.

60. Article 39 of the proposed Directive specifies that the period of retention for CDD personal data will be five years after the business relationship between the obliged entities and the customer has ended. Likewise, Article 16 of the proposed Regulation specifies that the period of retention will be five years after the payment has happened. Both articles further add that the retention period may be extended if provided for by national legislation "only if necessary for the prevention, detection or investigation of money laundering and terrorist financing. The maximum retention period after the business relationship has ended shall not exceed ten years".

61. The EDPS observes that the maximum potential retention period of ten years is too general. He therefore recommends that:
    - the criterion for the necessity of any extension of the retention period is specified and/or procedural safeguards are added to ensure that retention periods longer than 5 years are only applied in exceptional situations, and that the extension should be read as a maximum of five additional years;
    - the Proposals lay down that data may not be retained after the expiry of the retention period, regardless of national law;
    - the length of the retention period chosen is justified on a case by case basis. A recital should make clear that, if the retention period appeared to have been chosen in an arbitrary manner, without any clear link with professional or practical obligations, it would fail to comply with the requirements of Directive 95/46/EC.

[37] See Article 6(d) of Directive 95/46/EC.

3. SPECIFIC COMMENTS ON THE PROPOSALS

3.1. Specific comments on the proposed Directive

3.1.1. Limitation of data subjects' rights

62. Considering the potentially highly intrusive nature of AML obligations, the right of data subjects to be informed and the modalities of possible restrictions to data subjects' rights should be clearly elaborated in the proposed Directive. Furthermore, any restriction to the fundamental rights of individuals should be justified and proportionate. The EDPS recalls that the right of access is a core element of the fundamental right to data protection, which is expressly mentioned in Article 8 of the Charter of the Fundamental Rights of the Union. Exceptions therefore need to be interpreted in a restrictive way.

63. The EDPS suggests complementing the proposed Directive with a provision specifying who will be responsible for data subjects' information: he would favour an obligation for the obliged entities to inform the customer at the same time he/she is informed about general terms and conditions of the client/provider relationship.

64. Besides, Article 38(1) of the proposed Directive lays down a general derogation to the right of access. The EDPS notes that the only justification is given in recital 34 that refers to the limitation of data subjects' rights pursuant to Article 13 of Directive 95/46/EC, which is needed here in order to avoid the risk of seriously undermining the effectiveness of the fight against money laundering and terrorist financing. Moreover, the wording of the exception relating to Suspicious Transactions Reports (STRs) in Article 38(1) is very broad.

65. Moreover, Article 38(1) does not contain the required safeguards. The provision contains a general prohibition from providing information to data subjects, which is not circumscribed within any time limit. Given the possible consequences of the investigations carried out in the context of AML for data subjects, including the impossibility to establish a commercial relationship and, as a result, to open a bank account, it is disproportionate to introduce such a blanket prohibition without any time limit. Furthermore, it seems also disproportionate to limit the access rights in relation to those STRs which are, subsequently, considered unfounded or irrelevant. It would be hardly justifiable to limit access rights of the data subjects once it has been established that the STR is irrelevant or not founded, as the disclosure would not hamper any 'prevention, investigation, detection [or] prosecution' of possible criminal offences. Finally, it is not clear how the obliged entities, directors and employees are supposed to know whether an investigation 'may be carried out' by the competent authorities, given that normally investigations by law enforcement bodies are supposed to remain secret and confidential. The provision does not give any indication of which person or entity is responsible to establish whether an investigation 'may be carried out'.

66. The EDPS recommends that the proposed Directive specifies in more details in a substantive dedicated provision the conditions under which the data subjects´ rights may be limited and the objective pursued. Besides, he recommends

introducing the following time limits and conditions: if, after a certain period after the reporting to the FIU, it has been decided not to carry out an enquiry or that the alert given has not proven to be relevant, and provided that the individual concerned does not raise any suspicion, the data subject should be informed that a verification has been carried out and be able to exercise his/her rights of access and rectification. He also recommends adding an obligation for FIUs to inform the obliged entities if a report is not followed by an investigation.

3.1.2. Risk assessment

67. The proposed Directive creates obligations for Member States to carry out risk assessments to enable Member States to identify, understand and mitigate their own risks (see recitals 15, 16 and 17 and Section 2 of the Proposal, Articles 7 and 8).

68. However, notwithstanding the legitimacy and the necessity of these risks assessments, it is not specified in the text whether the assessment should involve personal data or not. This ambiguity appears in particular in Article 8(1), which indicates that the risk assessment by obliged entities must take into account "risk factors including *customers*, countries or geographic areas, products, *services*, *transactions* or delivery channels". This list seems to suggest that processing of personal data cannot be categorically excluded in the preparation of risk assessments.

69. Therefore, the EDPS recommends stating clearly whether or not risk assessments carried out by the designated authority and by obliged entities may involve the processing of personal data.

70. If personal data processing is envisaged, the proposed Directive should require the Member States to introduce the necessary data protection safeguards pursuant to their respective national laws. Amongst others, Member States will have to (i) identify the purpose of the processing operations and establish which are the compatible uses; (ii) identify and strictly limit which entities will have access to these risk assessments (the Commission, EBA, ESMA and EIOPA upon request); (iii) ensure the right of access and appropriate information for all the data subjects whose personal data may be processed and (iv) define and limit the retention period for the personal data to the minimum necessary for the performance of such purpose. Further retention of risk assessments would for instance be possible after complete anonymisation.

71. Pursuant to Article 7(5), the results of the risk assessment carried out by the designated authority should be made available to the Commission, EBA, ESMA and EIOPA upon request. Also in this case, if these reports involve processing of personal data, their processing would be subject to Regulation (EC) No 45/2001.

3.1.3. Customer due diligence

Specifying the data that can be collected to carry out customer due diligence to prevent arbitrary decisions and discrimination

72. Recitals 19, 20, 23 and 47 and Chapter II (Articles 9 to 28) of the proposed Directive address the issue of Customer Due Diligence (CDD) which can be simplified, enhanced or performed by third parties.

73. This subject is dealt with in a rather detailed manner and the circumstances when CDD is to be conducted are clearly stated (Articles 9 and 10). All obliged entities (for instance, credit and financial institutions, auditors, legal professionals, real estate agents, providers of gambling services (Article 2)) are asked to carry out this scrutiny on their customers. However, the concrete content of the scrutiny and the data that should be collected on a client when carrying out a CDD (also in relation to the enhanced or simplified CDD) are not sufficiently specified in the proposed Directive which leaves a broad margin of manoeuvre to the entities carrying out this scrutiny, which could lead to arbitrary and/or excessive processing of personal data if not to the processing of sensitive data.

74. The results of this scrutiny can deprive some people of, for instance, the possibility to open a bank account or establish a business relationship. The EDPS therefore welcomes the fact that recital 47 makes reference to the non discrimination principle enshrined in Article 21 of the EU Charter of Fundamental Rights. However, this reference does not give sufficient indication about which type of data can be or cannot be processed during the CDD[38].

75. The EDPS considers important to introduce in the text of the proposed Directive a precise list of the information that should and should not be taken into account in carrying out the CDD (including whether or not it would include sensitive data, as explained further below). In addition, the EDPS recommends the use of templates with answers to be given to multiple choice questions as they would prevent any subjective decision and ensure a harmonised application of the obligation throughout the EU. Specifications for such templates could be provided in implementing acts or in guidelines.

76. If this approach cannot be followed, the proposed Directive should at least include an obligation for the Member States to specify which data should or should not be collected by the obliged entities while carrying out the Customer Due Diligence. However, the EDPS wishes to emphasize the risk of legal uncertainty and incoherence between Member States that could derive from the absence of harmonized rules at the European level.

Sensitive data

77. It should be underlined that the processing of sensitive data as described in Article 8(1) of Directive 95/46/EC does not seem necessary for the purpose to be achieved by the proposed Directive. The text itself does not mention the necessity of such a processing. It cannot however be excluded that (in view of the definition of "criminal activity" in Article 3) during the CDD the obliged entities are to process sensitive data such as data related to offences or suspected offenses, criminal convictions or security measures of customers within the meaning of

[38] Annexes II and III only identify risk factors in general.

Article 8(5) of Directive 95/46/EC[39]. In this case, the latter Directive requires that the processing can only be allowed if it is carried out 'under the control of official authority, or if suitable specific safeguards are provided under national law [...]'. However, the proposed Directive does not address this issue.

78. Besides, the circumstances in which a CDD must be carried out may lead to discrimination if sensitive data are processed without limitation. Leaving it to obliged entities to decide whether they need sensitive data or not to carry out CDD involves the risk for them to take arbitrary decisions such as depriving clients of a certain ethnic origin that they consider to be suspect, or clients that have different political or religious opinions, of the right to conduct transactions.

79. The EDPS considers it necessary to clarify in the proposed Directive whether or not sensitive data within the meaning of Article 8(1) of Directive 95/46/EC should be collected for the purpose of carrying out the CDD. If such a processing were to be necessary, Member States should ensure that it is carried out under the control of an official authority and that suitable specific safeguards are provided under national law.

Enhanced due diligence

80. In cases identified in Articles 17 to 23 of the proposed Directive, and, in other cases of higher risks identified by Member States or obliged entities, enhanced customer due diligence will have to be applied. In particular, in cases where a banking/transaction relationship involves a respondent institution from a third country, a domestic or foreign politically exposed person[40] or a person who is or has been entrusted with a prominent function by an international organisation. Enhanced due diligence is defined in Article 16(2) as the obligation to "*examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose"*. Articles 18 and 19 provide for the setting up of "*appropriate risk-based procedures"*, obtaining "*senior management approval for establishing or continuing the business relationship"* and conducting "*enhanced ongoing monitoring of the business relationship"*.

81. The text specifies that in case of enhanced due diligence, also immediate family members and persons known to be close associates of politically exposed persons could be subjected to this scrutiny (Article 21). The EDPS notes that Article 21 could lead to an extensive scrutiny of the business and financial activities of

[39] In this regard, the EDPS wishes to recall that he considers that data relating to suspected offenses qualify as sensitive data under Article 8 of Directive 95/46/EC since they may cause people to be brought to civil or even criminal courts. See in particular opinion on credit rating agencies http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-02-09_EU_US_Joint_Customs_EN.pdf , in particular para 22 and also Opinion on ACTA http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf, para 32(ii).

[40] Article 3(7)(a) defines "*foreign politically exposed persons*" as *"natural persons who are or have been entrusted with prominent public functions by a third country"* and "*domestic politically exposed persons"* as *"natural persons who are or who have been entrusted by a Member State with prominent public functions"*.

family members or known close associates. Therefore, he recommends limiting more clearly the situations in which the risks are so substantial that they justify enhanced due diligence, and also including procedural safeguards against abuse.

3.1.4. Confidentiality and data protection

82. Article 42 requires Member States to ensure that the obliged entities take appropriate measures so that employees are aware of the provisions in force, including the relevant data protection requirements. Such measures should include special training programmes (Article 43). Article 45(2) requires Member States to ensure that staff of the national competent authorities maintains high professional standards of confidentiality and data protection. The EDPS welcomes these provisions which highlight the need for employees dealing with personal information on money laundering to respect data protection principles. He suggests that Article 42 also refers to confidentiality, given that the relevant employees will be involved in the CDD procedures.

3.1.5. Information on the beneficial owner

83. Article 29 states that 'Member States shall ensure that corporate or legal entities established within their territory obtain and hold adequate, accurate and current information on their beneficial ownership' without specifying which data should or should not be collected on the beneficial owner. On the contrary, Article 30, dealing with the trustees, states that the following data should be processed: identity of the settlor, the trustee(s), the protector (if relevant), the beneficiaries or class of beneficiaries, and any other natural person exercising effective control over the trust. The only (very general) information given in the proposed Directive on the data that should be collected when respecting this obligation is in recital 10, which recalls the 'need to identify any natural person who exercises ownership or control over a legal person'.

84. Since data that allow identifying a natural person can be the name, as well as some biometric data or an identification number, more specification is needed. The EDPS therefore recommends listing in a substantive provision of the proposed Directive which identification data should be collected on the beneficial owner, also when no trust is involved or, at the very least, introducing an obligation for the Member States to issue precise rules as to which data should or should not be collected by the obliged entities on the beneficial owner.

3.1.6. Cooperation and exchange of information between FIUs

85. The proposed Directive encourages cooperation and communication between FIUs (Subsection III, Articles 48 to 54). Cooperation with each other necessarily entails exchanges of information and therefore possibly relevant personal data of clients suspected of money laundering or terrorist financing. Recitals 39 and 40 promote better coordination and cooperation between Member States´ FIUs, particularly *via* secure facilities for the exchange of information, such as the decentralised computer network "*FIU.net*" and the techniques offered via this tool.

86. Given the nature of the personal data involved in the envisaged exchanges (in particular, considering that data about suspicions of offences[41] will be collected), specific security and privacy safeguards should be applied. The EDPS welcomes that Article 52 requires Member States to ensure that FIUs take all necessary measures, including security measures, and that information exchanged between FIUs is not made accessible to any other authority agency or department, unless prior approval is given by the FIU providing the information.

87. The EDPS also welcomes the specific requirement for Member States to require FIUs to apply 'sophisticated technologies' that would allow them to match their data with other FIUs in an anonymous way by ensuring 'full protection of personal data' (Article 53(1)). However, he suggests replacing the word "sophisticated technologies" by "state of the art technologies implementing privacy by design". The EDPS also recommends that (i) the retention period of the data exchange is defined and limited to what is strictly necessary in relation to the purpose of the processing, (ii) the update of data is ensured by designating agents responsible for it inside FIUs, and (iii) the way to ensure security of data processed is specified.

3.2. Specific comments on the proposed Regulation

3.2.1. Information collected on the payer and the payee

88. Pursuant to Article 4 of the proposed Regulation, *PSPs* should generally include the full name and the account number of the payer and the payee on all wire transfers, as well as the residential address of the payer. Each time an individual in the EU transfers money to a foreign country, this person's personal information will be sent along to the receiving PSP including full name, residential address or place and date of birth or national identity number, and transaction number.

89. The EDPS welcomes that Article 4 specifies which data should be collected both on the payer and the beneficiary, in accordance with the data minimization principle (Article 6(c) of Directive 95/46).

90. However, he questions the inclusion in that list of the national identity number and recalls that Article 8(7) of Directive 95/46/EC states that "*Member States shall determine the conditions under which a national identification number or any other identifier or general application may be processed"*. The EDPS underlines that the processing of the national identity number is subject to specific restrictions and/or safeguards in several Member States. He would therefore recommend using the transaction number instead. If this was not an option, it should be specified in Article 4 of the FTR that the inclusion of the national identity number in the data transferred to the receiving PSP is subject to stricter national legislation implementing Article 8(7) of Directive 95/46/EC.

91. The principle of data accuracy set forth in Article 6(d) of Directive 95/46/EC makes it necessary to verify that the data processed is correct and that no spelling mistake or confusion is made. Besides, identity theft is a concern that is often related to money laundering. Therefore, the EDPS wishes to highlight the

[41] See above para. 87 and footnote 45.

necessity for the PSPs to verify the information on the beneficiary of a transaction before reporting it[42], and welcomes in this context the specification in recital 14. Considering the high potential of inaccuracy of the data and the fact that it is the payment service provider's responsibility to ensure that he provides data that is accurate, the EDPS also welcomes that Articles 4(3), 4(4), 7 and 12 set up a verification procedure to ensure that the data is complete, but also that it is accurate.

3.2.2. Access to information / confidentiality

92. Articles 16 and 17 of Directive 95/46/EC require that guarantees are set up to ensure data confidentiality and security. Thus, individuals accessing the data must not process them except on instructions from the controller and appropriate technical and organizational measures must be implemented to protect data against accidental or unlawful destruction, accidental loss, alteration, unlawful disclosure etc. Confidentiality also implies that only persons who "need to know", i.e. individuals who need to access the data to exercise their professional responsibilities, should be able to access it.

93. In this regard, the EDPS notes that the confidentiality of the data is not mentioned in the proposed Regulation. Considering the high amount of data that will be processed as a result of the proposed Regulation and the high sensitivity of the context, the EDPS would favour the introduction of a provision stating that "the information should only be accessible to designated persons or classes of persons". He recommends that this newly introduced provision requires Member States to specify in national law the function the person needs to have within the organisation in order to be able to access the data.

94. The EDPS also notes that no provision ensures that the obliged entities take appropriate measures so that employees are aware of the relevant data protection requirements and, in particular, confidentiality and security requirements (similarly to what is set forth in Articles 42 and 45(2) of the proposed Directive). The EDPS therefore recommends inserting a provision highlighting the need for employees dealing with personal information on the payer and the payee to respect the confidentiality of the data processed as well as data protection requirements. Besides, this provision should also require Member States to ensure that a specific training is given to employees who will have to regularly collect personal data, and that guidelines reminding them of what they may or may not do, in particular which data they can or cannot process, in this context, are circulated.

3.2.3. Cooperation obligations

95. Article 15 states the obligation for PSPs to promptly respond to requests for information on the payer from the authorities responsible for combating money laundering or terrorist financing in the Member State and recital 20 underlines the necessity to do so. Given the nature of the personal data involved in the envisaged exchanges, safeguards should be applied. This includes both security and privacy requirements that authorities to whom the data will be transferred must respect.

[42]The importance of this accuracy check is stressed by the study on the application of the Regulation on information accompanying transfers of funds, MARKT/2011/054/F, page 97.

The authorities should also be reminded that the information exchanged should not be made accessible to any other authority agency or department that would not be allowed to access it. Therefore, the EDPS suggests adding a sentence in Article 15 that could read: “Specific safeguards should be put in place in order to ensure that such exchanges of information respect data protection requirements”.

96. The EDPS notes that Article 15 implies that authorities responsible for combating money laundering or terrorist financing in the Member State are amongst third parties who can access the data collected, upon presentation of a request. He recommends complementing Article 15 to ensure that no other external authorities or party that have no interest in combating money laundering or terrorist financing should access the data stored.

3.2.4. Reporting of breaches

97. The EDPS notes that Article 21 obliges Member States to establish effective mechanisms to encourage reporting of breaches of the provisions of this Regulation. He welcomes Article 21(2)(c) stating that these mechanisms shall include protection of personal data concerning the persons who report 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. However, he suggests that the provision be completed to specify to which authority the breaches will be reported and to require that appropriate technical and organizational measures are implemented to protect data against accidental or unlawful destruction, accidental loss, alteration, or unlawful disclosure.

4. CONCLUSIONS

98. The EDPS recognises the importance of anti money laundering policies for the economic and financial reputation of Member States. However, he underlines that the legitimate aim of achieving transparency of payments sources, funds deposits and transfers for purpose of countering terrorism and money laundering has to be pursued while ensuring compliance with data protection requirements.

99. The following issues should be addressed in both Proposals:
- an explicit reference to applicable EU data protection law should be inserted in both Proposals in a substantive and dedicated provision, mentioning in particular Directive 95/46/EC and the national laws implementing Directive 95/46/EC, and Regulation (EC) No 45/2001 as concerns the processing of personal data by EU institutions and bodies. This provision should also clearly state that the Proposals are without prejudice to the applicable data protection laws. The reference in recital 33 to Council Framework Decision 2008/977/JHA of 27 November 2008 should be deleted;
- a definition of "competent authorities" and "FIUs" should be added in the proposed Directive. This definition should guarantee that "competent authorities" are not to be considered as "competent authorities" within the meaning of Article 2(h) of the Framework Decision 2008/977/JHA.
- it should be clarified in recital 32 that the legal ground for the processing would be the necessity to comply with a legal obligation by the obliged

entities, competent authorities and FIUs (Article 7(c) of Directive 95/46/EC);

- it should be recalled that the sole purpose of the processing must be the prevention of money laundering and terrorist financing, and that data must not be further processed for incompatible purposes;
- the specific prohibition to process data for commercial purposes, which is currently mentioned in recital 31 of the proposed Directive and recital 7 of the proposed Regulation, should be laid down in a substantive provision;
- a dedicated recital should be added to clarify that the fight against tax evasion is only inserted as predicate offences;
- as to international transfers, dedicated substantive provisions on the transfers of personal data should be added, which provides for an appropriate legal basis for the intra-group/PSP to PSP transfers that would respect the text and interpretation of Article 26 of Directive 95/46/EC, as supported by the Article 29 Working Party of European data protection authorities. The EDPS recommends that the proportionality of requiring the mass transfer of personal and sensitive information to foreign countries for the purpose of fighting AML/TF is re-assessed and that a more proportionate approach is favoured;
- regarding the publication of sanctions, the EDPS recommends evaluating alternative and less intrusive options to the general publication obligation and, in any case, specifying in the proposed Directive:
  - the purpose of such a publication if it was to be maintained;
  - the personal data that should be published;
  - that data subjects are to be informed before the publication of the decision and are guaranteed rights to appeal this decision before the publication is carried out;
  - that data subjects have the right to object under Article 14 of Directive 95/46/EC on compelling legitimate grounds;
  - additional limitations relating to the publication online;
- as to data retention, a substantive provision should be added that sets forth a maximum retention period that must be respected by Member States, with additional specifications.

100. In respect of the proposed Directive, the EDPS further recommends to:

- add a specific provision to recall the principle of providing data subjects with information about the processing of their personal data (in accordance with Articles 10 and 11 of Directive 95/46/EC) and to specify who will be responsible for such data subjects' information;
- respect the proportionality principle when limiting data subjects' rights and, as a consequence, add a specific provision to specify the conditions under which the data subjects´ rights may be limited;
- clearly state whether or not risk assessments carried out by the designated authority and by obliged entities may involve the processing of personal data. If so, the proposed Directive should require the introduction of the necessary data protection safeguards;
- add a precise list of the information that should and should not be taken into account in carrying out the Customer Due Diligence. Clarify whether or not sensitive data within the meaning of Article 8(1) of Directive 95/46/EC

should be collected for this purpose. If such a processing were to be necessary, Member States should ensure that it is carried out under the control of an official authority and that suitable specific safeguards are provided under national law;

- amend Article 21 to limit more clearly the situations in which the risks are so substantial that they justify enhanced due diligence and to provide for procedural safeguards against abuse;
- amend Article 42 to include a reference to confidentiality, which should be respected by all employees involved in the CDD procedures;
- list in a substantive provision the types of identification data to be collected on the beneficial owner, also when no trust is involved.

101. In respect of the proposed Regulation, the EDPS further recommends to:

- refrain from using the national identity number as a reference without specific restrictions and/or safeguards, but to use the transaction number instead;
- recall the importance of respecting the principle of data accuracy, set forth in Article 6(d) of Directive 95/46/EC, in the context of AML procedures;
- add a provision stating that "the information should only be accessible to designated persons or classes of persons";
- add a provision regarding the respect of confidentiality and data protection obligations by employees dealing with personal information on the payer and the payee;
- clarify in Article 15 that no other external authorities or parties that have no interest in combating money laundering or terrorist financing should access the data stored;
- complete Article 21 by specifying to which authority the breaches of the Regulation will be reported and by requiring that appropriate technical and organizational measures are implemented to protect data against accidental or unlawful destruction, accidental loss, alteration, or unlawful disclosure.

Done in Brussels, 4 July 2013

(**signed**)

Giovanni BUTTARELLI
European Data Protection Assistant Supervisor