I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor 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

(2012/C 147/01)

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. This Opinion is part of a package of 4 EDPS' Opinions relating to the financial sector, all adopted on the same day [3].

2. On 20 October 2011, the Commission adopted a proposal 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 [4] (the 'proposed Directive') and a proposal for a Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation (EMIR) on OTC derivatives, central counterparties and trade repositories (the 'proposed Regulation') (both texts hereinafter jointly referred to as 'the Proposals').

3. The EDPS was informally consulted prior to the adoption of the proposals. The EDPS notes that several of his comments have been taken into account in the proposals.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] EDPS Opinions of 10 February 2012 on the legislative package on the revision of the banking legislation, credit rating agencies, markets in financial instruments (MIFID/MIFIR) and market abuse.
[4] OJ L 145, 30.4.2004, p. 1.

1.2. **Objective and scope of the proposals**

4. The Markets in Financial Instruments Directive ('MiFID'), in force since November 2007, is a core pillar in EU financial market integration. It currently consists of a framework Directive (Directive 2004/39/EC), an implementing Directive (Directive 2006/73/EC) and an implementing Regulation (Regulation (EC) No 1287/2006).

5. MiFID establishes a regulatory framework for the provision of investment services in financial instruments (such as brokerage, advice, dealing, portfolio management, underwriting etc.) by banks and investment firms and for the operation of regulated markets by market operators. It also establishes the powers and duties of national competent authorities in relation to these activities. Concretely, it abolishes the possibility for Member States to require all trading in financial instruments to take place only on specific exchanges and enables Europe-wide competition between traditional exchanges and alternative venues.

6. After more than three years in force, more competition between venues in the trading of financial instruments and more choice for investors in terms of services providers and available financial instruments have emerged. However, some problems also have surfaced. For instance, the benefits from the increased competition have not flowed equally to all market participants and have not always been passed on to the end investors, retail or wholesale, market and technological developments have outpaced various provisions in MiFID and the financial crisis has exposed weakness in the regulation of certain instruments.

7. The aim of the MiFID revision is to adapt and update the current rules to the market developments, including the financial crisis and technological development and improve their effectiveness.

1.3. **Aim of the EDPS Opinion**

8. Several aspects of the proposals have an impact on the rights of individuals relating to the processing of their personal data. These are: 1. obligations to keep records and transaction reporting; 2. powers of competent authorities (including power to inspect and power to require telephone and data traffic); 3. publication of sanctions; 4. reporting of violations, and in particular provisions on whistle-blowing; 5. cooperation between competent authorities of Member States and the ESMA.

2. **ANALYSIS OF THE PROPOSALS**

2.1. **Applicability of data protection legislation**

9. Several recitals ([5]) of the proposals mention the Charter of Fundamental Rights, Directive 95/46/EC and Regulation (EC) No 45/2001. However, a reference to the applicable data protection legislation should be inserted in a substantive article of the proposals.

10. A good example of such 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 ([6]), which explicitly provides as a general rule that Directive 95/46/EC and Regulation (EC) No 45/2001 apply to the processing of personal data within the framework of the proposal. The EDPS recently issued an Opinion on this proposal where he very much welcomes this overarching provision. However, the EDPS suggests that the reference to Directive 95/46/EC be clarified by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC.

11. The EDPS therefore suggests inserting a similar substantive provision as in Article 22 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation ([7]), subject to the suggestions he made on this proposal ([8]), i.e. emphasising the applicability of existing data protection legislation and clarifying the reference to Directive 95/46/EC by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC.

([5]) See recitals 20, 30 and 45 of the proposed Regulation and recitals 41, 43, 69 and 103 of the proposed Directive.
([6]) COM(2011) 651.
([7]) Commission proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, COM(2011) 651.
([8]) See EDPS Opinion of 10 February 2012 on the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, COM(2011) 651.

12. The recitals should also consistently use the wording that Member States 'shall' and not only 'should' respect the relevant data protection legislation, as the latter is in force and there is no discretion as regards its applicability.

2.2. **Obligation to keep records and transaction reporting**

2.2.1. *Obligation under the proposed Regulation*

13. Recital 27 and Articles 21 to 23 of the proposed Regulation introduce the principle according to which competent authorities coordinated by ESMA shall monitor the activities of investment firms to ensure that they act honestly, fairly and professionally and in a manner which promotes the integrity of the market. To do so, the authorities should be able to identify the person who has made the investment decision, as well as those responsible for its execution (recital 28).

14. In order to implement this monitoring activity, Article 22 obliges investment firms to keep at the disposal of the competent authority, for at least 5 years, the relevant data relating to all transactions in financial instruments which they have carried out. These records shall include all the information and details of the identity of the client. The details of transactions in financial instruments are to be reported to competent authorities to enable them to detect and investigate potential cases of market abuse, to monitor the fair and orderly functioning of markets, as well as the activities of investment firms. ESMA can also request access to these data.

15. The investment firm has to report details of these transactions, including the identity of the clients, to the competent authorities as quickly as possible (Article 23). If the clients involved are natural persons, these operations involve the processing of personal data within the meaning of Directive 95/46/EC and Regulation (EC) No 45/2001 and possibly the creation of general data bases.

16. The impact assessment does not seem to address the evaluation of the retention period of 5 years for the transaction reports. As Article 6(1)(e) of Directive 95/46/EC requires, personal data should not be kept for longer than it is necessary for the purpose for which the data were collected. In order to comply with this requirement, the EDPS suggests replacing the minimum retention period of 5 years with a maximum retention period. The chosen period should be necessary and proportionate for the purpose for which data have been collected.

2.2.2. *Obligation under the proposed Directive*

17. Article 16 of the Directive includes organisational requirements applicable to investment firms. In particular, the firms have to ensure that records of all services and transactions undertaken are kept, which would enable the relevant competent authorities to monitor compliance with the requirements under the Directive. Such records would allow verifying that the investment firm has complied with the obligations related to clients or potential clients. Although not specified in the text, it is to be assumed that such data would contain personal data of customers and employees.

18. The Commission is empowered by Article 16(12) to adopt delegated acts to specify the concrete organisational requirements spelled out in the Article. In this respect, the EDPS invites the Commission to consult him at the moment of the adoption of the delegated acts. In any case, such measures should aim at minimising the storing and processing of personal data to be recorded by the investment firms. As already noted in relation to the Regulation, the Commission should also thoroughly evaluate which retention period should be introduced for such data in order to make sure that the retention is adequate and proportionate.

2.3. **Duty to record telephone conversation or electronic communications**

19. According to the proposed Directive telephone conversations or electronic communications shall be recorded.

20. Records of telephone conversations or electronic communications normally contain personal data of the parties to the communication, even though they relate to financial transactions or professional activities. Data relating to electronic communications may convey a wide range of personal information, including traffic data but also content. Moreover, the use of the term 'conversation' implies that the content of the communications will be recorded.

21. As far as personal data within the meaning of Directive 95/46/EC and Regulation (EC) No 45/2001 are involved, the main data protection rules apply and in particular the principles of purpose limitation, necessity and proportionality and the obligation not to keep the data for longer than it is necessary.

Purpose limitation

22. According to Article 6.1(b) of the Directive 95/46/EC, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

23. Article 16.7 of the proposed Directive does not specify explicitly the purpose of the recording of the telephone conversations and electronic communications. However, several different purposes are referred to in Recital 42, Article 16.6 of the proposed Directive, in the CESR advice and the impact assessment.

24. Article 16.6 of the proposed Directive provides that an investment firm shall keep records of all services and transactions it undertaken 'in order to enable the competent authority to monitor compliance with the requirements of the proposed Directive and in particular, to ascertain that the investment firm has complied with all obligations with respect to clients or potential clients'.

25. Recital 42 of the proposed Directive explains that 'Recording of telephone conversations or electronic communications involving client orders (…) is justified in order to strengthen investor protection, to improve market surveillance and increase legal certainty in the interest of investment firms and their clients'. The recital also refers to the technical advice to the European Commission, released by the Committee of European Securities Regulators (CESR) on 29 July 2010 on the issue of the importance of such recordings ([9]).

26. The CESR advice highlights that, according to the competent authorities, recording of conversations would be necessary (i) to ensure that there is evidence to resolve disputes between an investment firm and its clients over the terms of transactions; (ii) to assist with supervisory work in relation to conduct of business rules; and (iii) to help deter and detect market abuse and to facilitate enforcement in this area. The recording would not be the only means to ensure supervision by the authorities, but it 'can help' to assist a competent authority to check compliance with, for example, the requirements in MiFID on information to clients and potential clients, on best execution and on client order handling.

27. The impact assessment explains that 'competent authorities need this information (i.e telephone and electronic recording) in order to ensure market integrity and enforcement of compliance with business of conduct rules' ([10]).

28. The different purposes referred to in Recital 42, Article 16.6 of the proposed Directive, CESR advice and the impact assessment are not described in a logical and consistent way, but are to be found in several places in the Proposal and side documents. According to Article 6.1 of Directive 95/46/EC, the data must be collected for specified, explicit and legitimate purposes. The EDPS therefore urges the legislator to clearly and precisely define the purpose of the recording of telephone conversations and electronic communications in Article 16.7 of the proposed Directive.

Necessity and proportionality

29. According to Article 6.1(c) of Directive 95/46/EC, personal data must adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, i.e. data collected have to be limited to what is appropriate to achieve the objective pursued and not go beyond what is necessary to achieve it.

([9]) CESR technical advice to the European Commission in the Context of the MiFID Review — Investor Protection and Intermediaries, 29 July 2010, CESR/10-417 p. 7, http://www.esma.europa.eu/system/files/10_417.pdf

([10]) Impact Assessment, page 150.

30. Article 16.7 refers to the telephone conversations or electronic communications including at least transactions concluded when dealing on own account and client orders when the services of reception and transmission of orders and execution on behalf of clients are provided.

31. Firstly, except for the transactions explicitly mentioned, Article 16.7 does not specify which telephone conversations and electronic communications the records are referring to. The EDPS understands that they concern communications related to the services and transactions undertaken by an investment firm. However this should clearly be specified. Furthermore the use of the terms 'including at least' leaves room for the recording of various series of telephone conversations or electronic communications. This provision should on the contrary clearly define the communications that will be recorded and limit them to those necessary for the purpose of the recording.

32. Secondly, the provision does not precise what categories of data will be kept. As already mentioned, data relating to electronic communications may convey a wide range of personal information, such as the identity of the persons making and receiving the communication, time indications, the network used, the geographic location of the user in case of portable devices, etc. This also implies possible access to the content of communications. Furthermore, the reference to the 'conversations' implies that the content of the communications will be recorded. In line with the principle of proportionality, personal data contained in records of telephone conversations and electronic communications must be limited to what is necessary for the purpose for which they have been collected.

33. If for instance the purpose of the recording of the communications is keeping evidence of the transactions, it seems that there would be no other alternatives but to record the content of the communications in order to be able to retrieve any evidence of the transactions. However, the recording of the content of the communications for the purposes of helping and detecting market abuse or for the general monitoring the compliance with the requirements under the proposed Directive would be excessive and disproportionate. In this respect, Article 71.2(d) of the proposed Directive which provides to the competent authority the power to require telephone and traffic data records held by an investment firm when there is a reasonable suspicion of a breach of the proposed Directive explicitly excludes the content of the communication. In a same way, Article 17.2(f) of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation ([11]) providing the same investigatory power to the competent authorities in order prove insider dealing or market manipulation also explicitly excludes the content of the communication.

34. The EDPS therefore strongly recommends specifying in Article 16.7 of the proposed Directive what kind of telephone conversations and electronic communications as well as the categories of data related to the conversations and communications will be recorded. Such data must be adequate, relevant and not excessive having regard to the same purpose.

Period of data retention

35. According to Article 6.1(e) of Directive 95/46/EC, personal data should be kept in a form which permits the identification of the data subjects for no longer than necessary for the purposes for which the data were collected ([12]). The retention period indicated in Article 16(7) is three years. The impact assessment recognizes that any measure in this field should respect EU data protection rules laid down in Directive 95/46/EC. However, it highlights that the retention period to be set should take account of existing EU legislation on retention of data generated or processed in connection with the provision of publicly available electronic communications for the purposes of fighting serious crime. It argues that this therefore maximum of three years has been found to comply with the principles of necessity and proportionality necessary to guarantee a lawful interference with a fundamental right ([13]).

([11]) COM(2011) 651 final.
([12]) Article 6(1)(e) of Directive 95/46/EC.
([13]) Impact assessment, page 150.

36. In the EDPS' view, the analysis on necessity and proportionality of the duration of the measure is not adequate. None of the different (and somewhat unclear) purposes for the recording of telephone conversations and electronic communications referred to in Article 16.6, Recital 42, the impact assessment or the CESR advice mention the fighting of serious crime.

37. The evaluation has to be made in accordance with the purposes of the recording in the framework of the proposed Directive. If for instance, the purpose is 'to ensure that there is evidence to resolve disputes between an investment firm and its clients over the terms of transactions' ([14]), then the impact assessment should evaluate how long data must be kept in relation to the statute of limitations of rights on the basis of which such disputes can be initiated.

38. The EDPS therefore invites the legislator to thoroughly evaluate which retention period is necessary for the purpose of the recording of telephone conversations and electronic communications within the specific scope of the proposal.

2.4. **Powers of competent authorities**

39. Article 71 of the Directive lists the supervisory and investigatory powers of the competent authorities.

40. Article 71(4) refers to Directive 95/46/EC, by stating that the processing of personal data collected in the exercise of the supervisory and investigatory powers shall in any event be carried out while respecting the fundamental rights to privacy and data protection. The EDPS welcomes this provisions which specifically addresses the connection between the role of authorities as investigators and the processing of personal data which is involved in their activities.

2.4.1. *The power to carry out on-site inspections*

41. Article 71(2)(c) provides for the competent authorities' power to carry out on-site inspections. Contrary to the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation ([15]) the present provision does not contain any reference to the power of the competent authorities to 'enter private premises in order to seize documents'. This might suggest that the inspection power is limited to the premises of investment firms and does not cover private premises. For the sake of clarity, the EDPS suggests clarifying this limitation expressly in the text. Should the Commission instead intend to allow inspection of private premises, the EDPS refers to the comment he made on this issue in his Opinion on the above mentioned proposal ([16]) according to which he considers that the general requirement of a prior judicial authorisation regardless of whether national law requires so would be justified in view of the potential intrusiveness of the power at stake.

2.4.2. *The power to request records of telephone and data traffic*

42. Article 71(2)(d) of the proposed Directive empowers competent authorities to 'require existing telephone and existing data traffic records held by investment firms'. It clarifies that the request is subject to the existence of a 'reasonable suspicion' that such records 'may be relevant to prove a breach by the investment firm of its obligations' under the Directive. In any case, the records shall not include 'the content of the communication to which they relate'. The EDPS appreciates that the text qualifies the powers of the competent authorities by requiring as a condition for access to the records the reasonable suspicion of a breach and by excluding access by the competent authorities to the content of the communications.

43. However, there is no definition of the notions of 'telephone and data traffic records' in the proposed Directive. Directive 2002/58/EC (ePrivacy Directive) only refers to 'traffic data' but not to 'telephone and data traffic records'. It goes without saying that the exact meaning of these notions determines the impact the investigative power may have on the privacy and data protection of the persons concerned. The EDPS suggests to use the terminology already in place in the definition of 'traffic data' in Directive 2002/58/EC.

([14]) See the CESR study mentioned in paragraph 26 above.
([15]) COM(2011) 651.
([16]) See recent EDPS Opinion of 10 February 2012 on the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation.

44. Data relating to use of electronic communication means may convey a wide range of personal information, such as the identity of the persons making and receiving the call, the time and duration of the call, the network used, the geographic location of the user in case of portable devices, etc. Some traffic data relating to internet and e-mail use (for example the list of websites visited) may in addition reveal important details of the content of the communication. Furthermore, processing of traffic data conflicts with the secrecy of correspondence. In view of this, Directive 2002/58/EC has established the principle that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication ([17]). According to Article 15.1 of this Directive, Member States may include derogations in national legislation for specific legitimate purposes, but they must be necessary, appropriate and proportionate within a democratic society to achieve these purposes ([18]).

45. The EDPS acknowledges that the aims pursued by the Commission in the CRA Regulation are legitimate. He understands the need for initiatives aiming at strengthening supervision of financial markets in order to preserve their soundness and better protect investors and economy at large. However, investigatory powers directly relating to traffic data, given their potentially intrusive nature, have to comply with the requirements of necessity and proportionality, i.e. they have to be limited to what is appropriate to achieve the objective pursued and not go beyond what is necessary to achieve it ([19]). It is therefore essential in this perspective that the provisions are clearly drafted regarding their personal and material scope as well as the circumstances in which and the conditions on which they can be used. Furthermore, adequate safeguards should be provided for against the risk of abuse.

46. Records of telephone and data traffic concerned will obviously involve personal data within the meaning of Directive 95/46/EC, Directive 2002/58/EC and Regulation (EC) No 45/2001. Therefore it should be assured that the conditions for fair and lawful processing of personal data, as laid down in the Directives and the Regulation, are fully respected.

47. The EDPS notes that Article 71(3) makes judicial authorisation obligatory whenever such authorisation is required by national law. However, the EDPS considers that a general requirement for prior judicial authorisation in all cases — regardless of whether national law requires so — would be justified in view of the potential intrusiveness of the power at stake and in the interest of harmonised application of legislation across all EU Member States. It should also be considered that various laws of the Member States provide for special guarantees on home inviolability against disproportionate and not carefully regulated inspections, searches or seizures especially when made by institutions of an administrative nature.

48. Moreover, the EDPS recommends introducing the requirement for ESMA to request records of telephone and data traffic by formal decision specifying the legal basis and the purpose of the request and what information is required, the time-limit within which the information is to be provided as well as the right of the addressee to have the decision reviewed by the Court of Justice.

49. The expression 'existing telephone and traffic data records' does not seem to be sufficiently clear. Telephone and data traffic records are not defined, although Article 71(2)(2) of the MiFID proposal specifies that they are only the ones 'held by investment firms'. Data held by investment firms are probably those indicated in Articles 16.6 and 16.7, commented above. This should mean that the text excludes records held by electronic communications providers that have a supply contract with the concerned investment firm. For the sake of clarity, the EDPS recommends clarifying to what telephone and traffic data records held by an investment firm are referring to.

([17]) See Article 6(1) of Directive 2002/58/EC (OJ L 201, 31.7.2002, p. 37).

([18]) Article 15.1 of Directive 2002/58/EC provides that such restrictions must 'constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e State security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13.1 of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph (…)'.

([19]) See, e.g., Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-92/09) v. Land Hessen*, not yet published in ECR, point 74.

2.5. **Publication of sanctions or other measures**

2.5.1. *Mandatory publication of sanctions*

50. Article 74 of the proposed Directive obliges Member States to ensure that the competent authorities publish *any* sanction or measure imposed for breach of the proposed Regulation or of the national provisions adopted in the implementation of the proposed Directive without undue delay, including information on the type and nature of the breach and the identity of persons responsible for it, unless such disclosure would seriously jeopardise the financial markets. This obligation is mitigated only where the publication would cause a 'disproportionate damage' to the parties involved, in which instance the competent authorities shall publish the sanctions on an anonymous basis.

51. The publication of sanctions would contribute to increase deterrence, as actual and potential perpetrators would be discouraged from committing offences to avoid significant reputational damage. Likewise it would increase transparency, as market operators would be made aware that a breach has been committed by a particular person ([20]). This obligation is mitigated only where the publication would cause a disproportionate damage to the parties involved, in which instance the competent authorities shall publish the sanctions on an anonymous basis. Furthermore, while acknowledging that introducing a sanctions regime (whether through a minimum or a full harmonization) would have an impact on fundamental rights such as Articles 7 (respect for private and family life) and 8 (protection of personal data) and potentially also on Articles 47 (right to an effective remedy and a fair trial) and 48 (presumption of innocence and right of defence) of the EU Charter ([21]), the impact assessment does not seem to explore the possible effects of the publication of sanctions themselves on those rights.

52. Under Article 75(2)(a), 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 ([22]). It is not clear how the publication obligation under Article 74 can be reconciled with the power to issue a public statement under Article 75(2)(a). The inclusion of the power to issue public statement in Article 75(2)(a) demonstrates that the publication is in itself a real sanction, which should be assessed on a case by case basis in light of the proportionality criteria enshrined in Article 76 ([23]).

53. The EDPS is not convinced that the mandatory publication of sanctions, as it is currently formulated, meets the requirements of data protection law as clarified by the Court of Justice in the *Schecke* judgment ([24]). He takes the view that the purpose, necessity and proportionality of the measure are not sufficiently established and that, in any event, adequate safeguards against the risks for the rights of the individuals should have been foreseen.

([20]) See the impact assessment report, p. 42 *et seq*.

([21]) See also page 43 — assessment of the impact on fundamental rights of the option 'minimum harmonization': 'Option interferes with Articles 7 (respect for private and family life) and 8 (protection of personal data) and potentially also with Articles 47 (right to an effective remedy and a fair trial) and 48 (presumption of innocence and right of defence) of the EU Charter. Option provides for limitation of these rights in law while respecting the essence of these rights. Limiting these rights is necessary to meet the general interest objective of ensuring compliance with MiFID rules to ensure fair and orderly trading and investor protection. In order to be lawful the administrative measures and sanctions which are imposed must be proportionate to the breach of the offence, respect the right not to be tried or punished twice for the same offence, the presumption of innocence, the right of defence, and the right to an effective remedy and fair trial in all circumstances […]'.

([22]) See the recent EDPS Opinion of 10 February 2012 on the proposal for a Directive on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms and a proposal for a Regulation on prudential requirements for credit institutions and investment firms.

([23]) 'Member States shall ensure that when determining the type of administrative sanctions or measures and the level of administrative pecuniary sanctions, the competent authorities shall take into account all relevant circumstances, including: (a) the gravity and the duration of the breach; (b) the degree of responsibility of the responsible natural or legal person; (c) the financial strength of the responsible natural or legal person, as indicated by the total turnover of the responsible legal person or the annual income of the responsible natural person; (d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined; (e) the losses for third parties caused by the breach, insofar as they can be determined; (f) the level of cooperation of the responsible natural or legal person with the competent authority; (g) previous violations by the responsible natural or legal person […]'.

([24]) Joined Cases C-92/09 and C-93/09, *Schecke*, paragraphs 56-64.

2.5.2. *Necessity and proportionality of the publication*

54. In the *Schecke* judgment, the Court of Justice annulled the provisions of a Council Regulation and a Commission Regulation requiring the mandatory publication of information concerning beneficiaries of agricultural funds, including the identity of the beneficiaries and the amounts received. The Court held that the said publication constituted the processing of personal data falling under Article 8(2) of the European Charter of Fundamental Rights (the 'Charter') and therefore an interference with the rights recognised by Articles 7 and 8 of the Charter.

55. After analysing that 'derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary', the Court went on to analyse the purpose of the publication and the proportionality thereof. It concluded that there was nothing to show that, when adopting the legislation concerned, the Council and the Commission took into consideration methods of publishing the information which would be consistent with the objective of such publication while at the same time causing less interference with those beneficiaries.

56. Article 74 of the proposed Directive seems to be affected by the same shortcomings highlighted by the ECJ in the *Schecke* judgment. It should be borne in mind that for assessing 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 ([25]).

57. After reading the proposal and the accompanying documents (i.e., the impact assessment report), the EDPS is under the impression that the purpose, and consequently the necessity, of this measure is not clearly established. While the recitals of the proposal are silent on these issues, the impact assessment report merely states that the 'publication of sanctions is an important element in ensuring that sanctions have a dissuasive effect on the addresses and is necessary to ensure that sanctions have a dissuasive effect on the general public' ([26]). Such a general statement does not appear sufficient to demonstrate the necessity of the measure proposed. If the general purpose is increasing deterrence, it seems that the Commission should have explained, in particular, why heavier financial penalties (or other sanctions not amounting to naming and shaming) would not have been sufficient.

58. Furthermore, the impact assessment report does not seem to sufficiently take into account less intrusive methods, such as publication limited to credit institutions or publication to be decided on a case by case basis. In particular the latter option would seem to be *prima facie* a more proportionate solution, especially if one considers that — as recognised in Article 75(2)(a) — publication is a sanction, which therefore is to be assessed on a case by case basis, taking account of the relevant circumstances, such the gravity of the breach, the degree of personal responsibility, recidivism, losses for third parties, etc. ([27]).

59. In the EDPS view, the possibility to assess the case in light of the specific circumstances makes this solution more proportionate and therefore a preferred option compared to mandatory publication in all cases. This discretion would, for example, enable the competent authority to avoid publication in cases of less serious violations, where the violation caused no significant harm, where the party has shown a cooperative attitude, etc.

60. Article 35(6) of the proposed Regulation concerns the publication on ESMA's website of a notice for any decision to impose or renew any limitation on the ability of a person to enter into a commodities derivatives contract. The identity of persons whose negotiating ability has been limited by ESMA is therefore to be published, alongside the applicable financial instruments, the relevant quantitative measures such as the maximum number of contracts the person or class of persons in question can enter into, and the reasons thereof. The entry into effect of the measure is bound to the publication itself (Article 35(7)). On the basis of the reasoning developed in relation to the provisions of the Directive, the EDPS encourages the legislator to consider whether publication is necessary and whether other less restrictive means exist in cases where natural persons are involved.

([25]) See also in this regard EDPS Opinion of 15 April 2011 on the Financial rules applicable to the annual budget of the Union (OJ C 215, 21.7.2011, p. 13).
([26]) See footnote 11 above.
([27]) I.e. in accordance with Article 74 of the proposed Directive laying down the criteria for the determination of sanctions.

2.5.3. *The need for adequate safeguards*

61. The proposed Directive should have foreseen adequate safeguards in order to ensure a fair balance between the different interests at stake. Firstly, safeguards are necessary in relation to the right of the accused persons to challenge the decision before a court and the presumption of innocence. Specific language ought to have been included in the text of Article 74 in this respect, so as to oblige competent authorities to take appropriate measures with regard to both the situations where the decision is subject to an appeal and where it is eventually annulled by a court ([28]).

62. Secondly, the proposed Directive should ensure that the rights of the data subjects are respected in a proactive manner. The EDPS appreciates the fact that the final version of the proposal foresees the possibility to exclude the publication in cases where it would cause disproportionate damage. However, a proactive approach should imply that data subjects are informed beforehand of the fact that the decision sanctioning them will be published, and that they are granted the right to object under Article 14 of Directive 95/46/EC on compelling legitimate grounds ([29]).

63. Thirdly, while the proposed Directive does not specify the medium on which the information should be published, in practice, it is imaginable that in most of the Member States the publication will take place in the Internet. Internet publications raise specific issues and risks concerning in particular the need to ensure that the information is kept online for no longer than is necessary and that the data cannot be manipulated or altered. The use of external search engines also entail 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 ([30]).

64. In view of the above, it is necessary to oblige Member States to ensure that personal data of the persons concerned are kept online only for a reasonable period of time, after which they are systematically deleted ([31]). Moreover, Member States should be required to ensure that adequate security measures and safeguards are put in place, especially to protect from the risks related to the use of external search engines ([32]).

2.5.4. *Conclusions on publication*

65. The EDPS is of the view that the provision on the mandatory publication of sanctions — as it is currently formulated — does not comply with the fundamental right to privacy and data protection. The legislator should carefully assess the necessity of the proposed system and verify whether the publication obligation goes beyond what is necessary to achieve the public interest objective pursued and whether there are not less restrictive measures to attain the same objective. Subject to the outcome of this proportionality test, the publication obligation should in any event be supported by adequate safeguards to ensure respect of the presumption of innocence, the right of the persons concerned to object, the security/accuracy of the data and their deletion after an adequate period of time.

2.6. **Reporting of breaches**

66. Article 77 of the proposed Directive deals with mechanisms for reporting breaches, also known as whistle-blowing schemes. While they may serve as an effective compliance tool, these systems raise significant issues from a data protection perspective ([33]). The EDPS welcomes the fact that the proposed

([28]) For example, the following measures could be considered by national authorities: to delay the publication until the appeal is rejected or, as suggested in the impact assessment report, to clearly indicate that the decision is still subject to appeal and that the individual is to be presumed innocent until the decision becomes final, to publish a rectification in cases where the decision is annulled by a court.

([29]) See EDPS Opinion of 10 April 2007 on the financing of the Common Agricultural Policy (OJ C 134, 16.6.2007, p. 1).

([30]) See in this regard the document published by the Italian DPA Personal Data As Also Contained in Records and Documents by Public Administrative Bodies: Guidelines for Their Processing by Public Bodies in Connection with Web-Based Communication and Dissemination, available on the website of the Italian DPA, http://www.garanteprivacy.it/garante/doc.jsp?ID=1803707

([31]) These concerns are also linked to the more general right to be forgotten, whose inclusion in the new legislative framework for the protection of personal data is under discussion.

([32]) These measures and safeguards may consist for instance of the exclusion of the data indexation by means of external search engines.

([33]) The Article 29 WP published an opinion on such schemes in 2006 dealing with the data protection related aspects of this phenomenon: Opinion 1/2006 on the application of EU data protection rules to internal whistle blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (WP Opinion on whistle blowing). The Opinion can be found on the Article 29 WP website: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

Directive contains specific safeguards, to be further developed at national level, concerning the protection of the persons reporting on the suspected violation and more in general the protection of personal data. The impact assessment mentions the whistle-blowing schemes as part of the options to introduce sanctions in the fundamental rights assessment ([34]) and recalls the attention to the need for implementing legislation to comply with data protection principles and criteria indicated by data protection authorities. The EDPS is conscious of the fact that the Directive only sets out the main elements of the scheme to be implemented by Member States. Nonetheless, he would like to draw the attention to the following additional points.

67. The EDPS highlights, as in the case of other opinions ([35]), the need to introduce a specific reference to the need to respect the confidentiality of whistleblowers' and informants' identity. The EDPS underlines that the position of whistleblowers is a sensitive one. Persons that provide such information should be guaranteed that their identity is kept confidential, in particular vis-à-vis the person about whom an alleged wrongdoing is being reported ([36]). The confidentiality of the identity of whistleblowers should be guaranteed at all stages of the procedure, so long as this does not contravene national rules regulating judicial procedures. In particular, the identity may need to be disclosed in the context of further investigation or subsequent judicial proceedings instigated as a result of the enquiry (including if it has been established that they maliciously made false statements about him/her) ([37]). In view of the above, the EDPS recommends to add in letter b of Article 77.1 the following provision: 'the identity of these persons should be guaranteed at all stages of the procedure, unless its disclosure is required by national law in the context of further investigation or subsequent judicial proceedings'.

68. The EDPS further highlights the importance of providing appropriate rules in order to safeguard the access rights of the accused persons, which are closely related to the rights of defence ([38]). The procedures for the receipt of the report and their follow-up referred to in Article 77.1(a) should ensure that the rights of defence of the accused persons, such as the right to be informed, right of access to the investigation file and presumption of innocence, are adequately respected and limited only to the extent necessary ([39]). The EDPS suggests in this regard to add also in the proposed Directive the provision of Article 29 letter d) of the Commission proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, which requires Member State to put in place 'appropriate procedures to ensure the right of the accused person of defence and to be heard before the adoption of a decision concerning him and the right to seek effective judicial remedy against any decision or measure concerning him'.

69. Finally, as regards letter c) of Article 77.1, the EDPS is pleased to see that this provision requires Member States to ensure the protection of personal data of both accused and the accusing person, in compliance with the principles laid down in Directive 95/46/EC. He suggests however removing 'the principles laid down in', to make the reference to the Directive more comprehensive and binding. As to the need to respect data protection legislation in the practical implementation of the schemes, the EDPS would like to underline in particular the recommendations made by the Article 29 Working Party in its 2006 Opinion on whistle-blowing. Among others, in implementing national schemes the entities concerned should bear in mind the need to respect proportionality by limiting, as far as possible,

([34]) See Impact Assessment, p. 137-138: 'Regarding the introduction of "whistle blowing schemes", this raises issues regarding the protection of personal data (Article 8 of the EU Charter and Article 16 of the TFEU) and the presumption of innocence and right of defence (Article 48) of the EU Charter. Therefore, any implementation of whistle blowing schemes should comply and integrate data protection principles and criteria indicated by EU data protection authorities and ensure safeguards in compliance with the Charter of fundamental rights '.

([35]) See for instance, the Opinion on financial rules applicable to the annual budget of the Union of 15 April 2011, and the opinion on investigations conducted by OLAF of 1 June 2011, both available at http://www.edps.europa.eu

([36]) The importance of keeping the identity of the whistleblower confidential has already been underlined by the EDPS in a letter to the European Ombudsman of 30 July 2010 in case 2010-0458, to be found on the EDPS website (http://www.edps.europa.eu). See also EDPS prior check Opinions of 23 June 2006, on OLAF internal investigations (Case 2005-0418), and of 4 October 2007 regarding OLAF external investigations (Cases 2007-47, 2007-48, 2007-49, 2007-50, 2007-72).

([37]) See Opinion on financial rules applicable to the annual budget of the Union 15 April 2011, available at http://www.edps.europa.eu

([38]) See in this regard EDPS Guidelines concerning the processing of personal data in administrative inquiries and disciplinary proceedings by European institutions and bodies, pointing out the close relationship between the right of access of the data subjects and the right of defence of the persons being accused (see p. 8 and 9) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-04-23_Guidelines_inquiries_EN.pdf

([39]) See Working Party 29 Opinion on whistle-blowing, p. 13-14.

the categories of persons entitled to report, the categories of persons who may be incriminated and the breaches for which they may be incriminated; the need to promote identified and confidential reports against anonymous reports; the need to provide for disclosure of the identity of whistleblowers where the whistleblower made malicious statements; and the need to comply with strict data retention periods.

2.7. **Cooperation between competent authorities of Member States and ESMA**

2.7.1. *Cooperation under the proposed Directive*

70. Article 83 introduces the obligation to cooperate between competent authorities of the Member States and between these and ESMA. In particular, paragraph 83(5) envisages an obligation for competent authorities to notify to ESMA and other authorities the details of (a) any request to any person who provided information on total exposure to take steps to reduce such exposure (pursuant to Article 72(1)(f)) and of (b) any limits on the ability of persons to enter into commodity contracts (pursuant to Article 72(1)(g)). The notification shall include the details regarding the identity of the person who is the addressee of such measures, as well as the scope of the limits, the type of financial instruments covered and other information.

71. Furthermore, it is provided that competent authorities of Member States which receive the above described notifications 'may take measures in accordance with Article 72(1)(f) or (g) where it is satisfied that the measure is necessary to achieve the objective of the other competent authority'. The EDPS would like to highlight that this type of decision to be taken by the competent authority might be interpreted as to be fulfilling the criteria of an 'automated individual decision' as described in Article 15 of Directive 95/46/EC: this interpretation is triggered by the fact that Article 72 requires the receiving competent authority to verify whether the measure at stake can achieve the objective of the *other* competent authority. The competent authority of the Member State receiving the notification is therefore not specifically required to carry out an independent analysis of the circumstances of the case — also based on personal data of the subject — in order to issue a measure which limits his rights. Article 15 of Directive 95/46/EC provides that every person should be granted the right not to be subject to a decision which produces legal effects concerning him or significantly affecting him and which is based solely on automated procession of data intended to evaluate certain personal aspects such as work performance, creditworthiness, reliability etc. For the context under examination, paragraph 15(2) of Directive 95/46/EC is relevant: it provides that a person may be subjected to a decision of the kind referred to above, if the decision 'is authorized by law' and safeguards to protect the data subject's legitimate interests are in place. The national laws implementing the Directive would constitute the legal basis for the exception of Article 15(2) of Directive 95/46/EC, however no specific safeguards are introduced to protect the data subjects' legitimate interests.

72. The text of the proposed Directive seems therefore to be introducing the possibility of an automated decision affecting the ability to conclude contracts by an authority based in a Member State different from the one in which the sanction was originally applied. Given the impact that such a decision can have on the rights of a person professionally engaged in investment activities, the EDPS highlights that the text should specifically introduce a reference to the right to object to automated individual decisions pursuant to Article 15 of Directive 95/46/EC. It should expressly introduce safeguards in order to guarantee that the data subject can be made aware of the transfer and of the existence of a process initiated by the receiving competent authority to adopt such a decision, in order to be able to effectively exercise the right to object.

2.7.2. *Cooperation under the proposed Regulation*

73. Article 34(2) of the Regulation establishes that after notification of any measure under Article 83(5) of the Directive, ESMA shall record the measure and the reasons thereof, and it shall maintain and publish on its website a database with summaries of the measures in force in relation to measures pursuant to Article 72(1) subparagraph (f) and (g) of the Directive, 'including details on the person or class of persons concerned'.

74. Such publication constitutes a further processing activity which involves personal data. The same observations raised in relation to the publication of sanctions in Chapter 2.5 above apply in this case. There seem to be no evaluation in the impact assessment of the impact on fundamental rights of this type of internet publication. The EDPS therefore encourages the legislator to reflect about the actual necessity and proportionality of this measure.

2.8. **Information exchanges with third countries**

75. The EPDS notes the reference to Directive 95/46/EC, particularly to Chapter 4 and the Regulation (EC) No 45/2001 in Article 92 of the proposed Directive.

76. However, in view of the risks concerned in such transfers the EDPS recommends adding specific safeguards such as the case-by-case assessment, the assurance of the necessity of the transfer, the requirement for prior express authorisation of the competent authority to a further transfer of data to and by a third country and the existence of an adequate level of protection of personal data in the third country receiving the personal data.

77. A good example of such a provision containing appropriate safeguards can be found in Article 23 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation ([40]).

3. **CONCLUSIONS**

78. The EDPS makes the following recommendations:

— insert a substantive provision in the proposals with the following wording: 'With regards to the processing of personal data carried out by Member States within the framework of this Regulation, competent authorities shall apply the provisions of national rules implementing Directive 95/46/EC. With regards to the processing of personal data carried out by ESMA within the framework of this Regulation, ESMA shall comply with the provisions of Regulation (EC) No 45/2001';

— replace in Article 22 of the proposed Regulation the minimum retention period of 5 years with a maximum retention period;

— specify in Article 16.7 of the proposed Directive (i) the purpose of the recording of telephone conversations and electronic communications and (ii) to what kind of telephone conversations and electronic communications it is referred toas well as the categories of data related to the conversations and communications will be recorded,

— clarify in Article 71.2(c) of the proposed Directive that the inspection power is limited to the premises of investment firms and does not cover private premises;

— introduce in Article 71.2(d) concerning the power to require telephone and traffic data, the prior judicial authorisation as a general requirement and the requirement of a formal decision specifying: (i) the legal basis (ii) the purpose of the request (iii) what information is required (iv) the time-limit within which the information is to be provided and (v) the right of the addressee to have the decision reviewed by the Court of Justice;

— clarify to what telephone and traffic data records Article 71.2(d) is referring to;

— in light of the doubts expressed in the present Opinion, assess the necessity and proportionality of the proposed system of mandatory publication of sanctions. Subject to the outcome of the necessity and proportionality test, in any event provide for adequate safeguards to ensure respect of the presumption of innocence, the right of the persons concerned to object, the security/accuracy of the data and their deletion after an adequate period of time;

([40]) Article 23 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation COM(2011) 651 states as follows:
'1. The competent authority of a Member State may transfer personal data to a third country provided the requirements of Directive 95/46/EC, particularly of Articles 25 or 26, are fulfilled and only on a case-by-case basis. The competent authority of the Member State shall ensure that the transfer is necessary for the purpose of this Regulation. The competent authority shall ensure that the third country does not transfer the data to another third country unless it is given express written authorisation and complies with the conditions specified by the competent authority of the Member State. Personal data may only be transferred to a third country which provides an adequate level of protection of personal data.
2. The competent authority of a Member State shall only disclose information received from a competent authority of another Member State to a competent authority of a third country where the competent authority of the Member State concerned has obtained express agreement of the competent authority which transmitted the information and, where applicable, the information is disclosed solely for the purposes for which that competent authority gave its agreement.
3. Where a cooperation agreement provides for the exchange of personal data, it shall comply with Directive 95/46/EC.'

— with regard to Article 77.1 (i) add in letter b) a provision saying that: 'the identity of these persons should be guaranteed at all stages of the procedure, unless its disclosure is required by national law in the context of further investigation or subsequent judicial proceedings'; (ii) add a letter d) requiring Member States to put in place 'appropriate procedures to ensure the right of the accused person of defence and to be heard before the adoption of a decision concerning him and the right to seek effective judicial remedy against any decision or measure concerning him'; (iii) remove 'the principles laid down' from letter c) of the provision.

Done at Brussels, 10 February 2012.

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor