I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Commission proposals for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, and for a Directive of the European Parliament and of the Council on criminal sanctions for insider dealing and market manipulation

(2012/C 177/01)

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 Regulation of the European Parliament and of the Council on insider dealing and market manipulation (the 'proposed Regulation') and a proposal for a Directive of the European Parliament and of the Council on criminal sanctions for insider dealing and market manipulation (the 'proposed Directive'). The proposed Regulation and Directive (jointly referred to as 'the proposals') were sent by the Commission to the EDPS for consultation and received on 31 October 2011. On 6 December 2011, the Council of the European Union consulted the EDPS on 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.

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

4. The EDPS welcomes that he is consulted by the Commission and the Council.

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

5. The Market Abuse Directive ('MAD') ([1]), adopted in early 2003, has introduced a common EU legal framework for preventing, detecting and imposing sanctions for both insider dealing and market manipulation.

6. After several years into force, the Commission has assessed the application of the MAD and has identified a number of problems like gaps in regulation of certain instruments and markets, deficiency of effective enforcement (regulators lack certain information and powers and sanctions are either lacking or insufficiently dissuasive), absence of clarity on certain key concepts and administrative burdens on issuers.

7. In light of these problems and of the important changes brought to the financial landscape through legislative, market and technological developments, the Commission has adopted legislative proposals for the reform of MAD which consist of the proposed Regulation and the proposed Directive. The policy objectives of the proposed revision are to increase investor confidence and market integrity and to keep pace with the new developments in the financial sector.

8. The proposed Regulation in particular extends the scope of the market abuse framework, qualifies attempts at market manipulation and attempted insider dealing as specific offences, strengthens the investigative powers granted to the competent authorities and introduces minimum rules for administrative measures, sanctions and fines.

9. The proposed Directive requires Member States to introduce criminal sanctions for intentional insider dealing or market manipulation and for inciting aiding and abetting or attempting to commit either offence. It also extends liability to legal persons, including, whenever possible, criminal liability of legal persons.

1.3. **Aim of the Opinion of the EDPS**

10. Several of the measures planned in the proposals to achieve the increasing of market integrity and investor protection impact upon the rights of individuals relating to the processing of their personal data.

11. In particular, when competent authorities investigate or cooperate in order to detect, report and/or sanction insider dealing or market abuse, personal data will be collected, processed and exchanged. Furthermore, the mechanism to encourage persons to report violations will also involve processing of personal data concerning both the person who reports the violations and the 'accused' person. Finally, the sanctioning regime will affect the right to the protection of personal data as far as sanctions mentioning the identity of the person responsible of the breach of the proposed Regulation will be published.

12. While the proposed Regulation contains several provisions that may affect the individual's right to protect their personal data, the proposed Directive does not as such involve processing of personal data. The present Opinion will therefore focus on the proposed Regulation and in particular on the following issues: 1. the applicability of data protection legislation; 2. the insider lists; 3. the powers of competent authorities; 4. the systems in place to detect and report suspicious transactions; 5. the exchange of information with third states; 6. the publication of sanctions and the reporting of violations.

([1]) Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse), OJ L 96, 12.4.2003, p. 16.

2. ANALYSIS OF THE PROPOSALS

2.1. Applicability of data protection legislation

13. Both recitals ([1]) and provisions ([2]) of the proposed Regulation mention the Charter of Fundamental Rights, Directive 95/46/EC and Regulation (EC) No 45/2001. In particular, Article 22 of the proposed Regulation explicitly provides as a general rule that 'with regard to the processing of personal data carried out by Member States within the framework of this Regulation, competent authorities shall apply the provisions of Directive 95/46/EC. With regard 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'. Furthermore, the provision provides for a maximum retention period of 5 years for personal data.

14. The EDPS very much welcomes this overarching provision and appreciates in general the attention specifically paid to the data protection legislation in the proposed Regulation. However, the EDPS suggests that the provision should be rephrased emphasising the applicability of existing data protection legislation. Moreover, the reference to Directive 95/46/EC should be clarified by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC. The EDPS notes that some provisions of the proposed Regulation explicitly refer to Directive 95/46/EC and/or Regulation (EC) No 45/2001. This highlights the application of the relevant data protection rules in specific cases, but does not imply that the rules are not applicable when not explicitly mentioned in every provision (potentially) involving processing of personal data.

15. As in recital 33, other recitals should 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. Insider lists

16. The proposed Regulation contains the obligation for issuers of a financial instrument or emission allowances market participants to draw up a list of all persons working for them, under a contract of employment or otherwise, who have access to inside information (Article 13.1). Issuers of a financial instrument whose financial instruments are admitted to trading on SME growth market are exempted of such obligation except when requested to do so by the competent authority (Article 13.2).

17. The EDPS acknowledges the necessity of such list as an important tool for competent authorities when investigating possible insider dealing or market abuse. However, as far as these lists will involve the processing of personal data, main data protection rules and guarantees should be laid down in the basic law. Therefore the EDPS recommends making an explicit reference to the purpose of such list in a substantive provision of the proposed Regulation. The purpose is indeed one of the essential elements of any processing according to Article 6 of Directive 95/46/EC.

18. According to Article 13.3 of the proposed Regulation, the Commission shall adopt, by means of delegated acts, measures determining the content of a list (including information as to the identities and the reasons for persons to be included on an insider lists) and the conditions under which such list will be drawn up (including the conditions for updating, the period of conservation and the responsibilities of the persons listed). However, the EDPS recommends:

— including the main elements of the list (in any event the reasons for persons to be included) in the proposed Regulation itself;

— including a reference to the need to consult the EDPS in so far as the delegated acts concern the processing of personal data.

2.3. Powers of the competent authorities.

19. Article 17.2 lists the supervisory and investigatory powers that the competent authorities shall at least have to fulfil their duties under the proposed Regulation.:

([1]) See recitals 33, 35, 39 and 40 of the proposed regulation.
([2]) See articles 17.4, 22, 23 and 29.1 (c) of the proposed regulation.

20. Two powers in particular need particular attention due to their interference with the rights of privacy and data protection: the power to enter private premises in order to seize documents in any form and the power to require existing telephone and data traffic records.:

2.3.1. *The power to enter private premises*

21. The power to enter private premises in order to seize documents in any form is highly intrusive and interferes with the right of privacy. It should therefore be subjected to strict conditions and surrounded with adequate safeguards ([1]). Article 17.2 (e) requires that access to private premises is submitted to prior authorization from the judicial authority in accordance with national law and to the existence of reasonable suspicion that documents related to the subject-matter of the inspection may be relevant to prove a case of insider dealing or market manipulation. The EDPS appreciates that the text qualifies the powers of the competent authorities by requiring as conditions to enter private premises the reasonable suspicion of a breach to the proposed Regulation or Directive and the prior authorisation from a judicial authority. However, the EDPS considers that the general requirement of a prior judicial authorisation regardless of whether national law so requires is both justified and required in view of the potential intrusiveness of the power at stake.

22. Recital 30 of the proposed Regulation specifies cases where access to private premises is necessary, i.e. the person to whom a demand for information has already been made fails (wholly or partly) to comply with or where there are reasonable grounds for believing that if a demand were to be made, it would not be complied with or that the documents or the information to which the information requirement relates, would be removed, tampered with or destroyed. The EDPS welcomes these specifications. However, he considers that they are additional safeguards, which are needed to ensure compliance with the right to privacy and that they should therefore be inserted in a substantive provision as a condition to access private premises.

2.3.2. *The power to require existing telephone and existing data traffic records*

23. Article 17.2 (f) empowers the competent authorities to 'require existing telephone and existing data traffic records held by a telecommunication operator or by an investment firm', however it clarifies that the request is subject to the existence of a 'reasonable suspicion' that such records 'may be relevant to prove insider dealing or market manipulation' under the proposed Regulation or the proposed Directive. These records shall however not include 'the content of the communication to which they relate'. Furthermore paragraph 3 of Article 17 provides that powers referred to in paragraph 2 shall be exercised in accordance with national law.

24. 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 ([2]) (the E-Privacy Directive) 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 ([3]). 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 ([4]).

([1]) See in particular ECHR, 23 February 1993, *Funcke* v. *France*, 10828/84.

([2]) Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37).

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

([4]) 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 (...)'.

25. The EDPS acknowledges that the aims pursued by the Commission in the proposed 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 ([1]). 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.

26. 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. Recital 31 of the proposed Regulation mentions that: 'telephone and data traffic records may establish the identity of a person responsible for the dissemination of false or misleading information, that persons have been in contact at a certain time, and that a relationship exists between two or more people ([2]).' 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. As long as this is the case, 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.

2.3.3. *Requirement of a judicial authorisation*

27. The EDPS notes that according to Article 17(3) this power shall be exercised in accordance with national law without explicitly referring to prior judicial authorisation, as is the case with regard to the power to enter private premises. 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.

28. Moreover, the EDPS recommends introducing the requirement for competent authorities 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.

2.3.4. *Definition of telephone and data traffic records*

29. There is no definition of the notions of 'telephone and data traffic records' in the proposed Regulation. Directive 2002/58 (ePrivacy) 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.

30. Article 17.2 (f) refers to 'existing telephone and data traffic records held by a telecommunication operator'. The E-Privacy Directive establishes the principle that traffic data must be deleted when it is no longer needed for the commercial purpose it was collected for. However, on the basis of Article 15.1 of E-Privacy Directive, Member States can derogate from this obligation for law enforcement purposes. The Data Retention Directive intends to align Member States' initiatives under Article 15(1) of E-privacy Directive, as far as it concerns retention of data for the investigation, detection and prosecution of 'serious' crime.

([1]) 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]) See also p. 12 of the explanatory memorandum of the proposed Regulation.

31. The question is whether telephone and data traffic records mentioned in Article 17.2 (f) refer to the data available through the storage of traffic and location data regulated by the E-Privacy Directive or to the additional data required by the Data Retention Directive. The latter option would raise serious concerns as derogations provided in Article 15.1 of E-Privacy Directive (i.e. the prevention, detection, investigation and prosecution of criminal offences) would be used to broaden the purposes for which data is retained under the Data Retention Directive (i.e investigation, detection and prosecution of 'serious' crime). In other words, the data which are retained under the Data Retention Directive would in this way be used for purposes that are not foreseen by this Directive. This would imply a European encouragement to use the 'legal loophole' which constitutes one of the main flaws of the current Data Retention Directive ([1]).

32. The EDPS therefore strongly recommends specifying the categories of telephone and data traffic records which competent authorities can require. Such data must be adequate, relevant, and not excessive in relation to the purpose for which they are accessed and processed. Furthermore, the EDPS recommends to limit Article 17.2 (f) to data normally processed ('held') by telecommunications operators in the framework of E-Privacy Directive 2002/58/EC. This excludes in principle access to data retained for the purposes of the Data Retention Directive, insofar as such access is not for the purpose of the investigation, detection and prosecution of 'serious' crimes ([2]).

33. Article 17.2 (f) provides for an access to 'telephone and traffic data records held by an investment firm'. The text should specify the categories of records and clarify the firms to whom the provision is referring to. The EDPS assumes that the records will coincide with the ones referred to in the proposal for a Directive of the European Parliament and of the Council on markets in financial instruments ('the proposed MIFID'). He stresses that he issued some observations on this proposal according which he recommended clarifying these notions as well ([3]). Moreover, as far as telephone and traffic data would concern the telephone conversations and electronic communications referred to in Article 16.7 of the proposed MiFID, the EDPS recommended defining the purpose of the recording of such communications and specifying what kind of communications as well as what categories of data of the communications will be recorded ([4]).

34. Finally, the EDPS is pleased to see that the text requires as a condition for access to the records the reasonable suspicion of a breach of the proposed Regulation or the proposed Directive and that it excludes explicitly access by the competent authorities to the content of the communications.

2.4. **Systems in place to detect and report suspicious transactions**

35. Paragraph 1 of Article 11.1 of the proposed Regulation foresees that any person who operates the business of a trading venue shall adopt and maintain effective arrangements and procedures aimed at preventing and detecting market abuse. Moreover, paragraph 2 requires that any person who is professionally arranging or executing transactions in financial instruments shall have systems in place to detect and report orders and transactions that might constitute insider dealing, market manipulation or an attempt to engage in market manipulation or insider dealing. In case of suspicion, the

([1]) See in this regard the EDPS Opinion of 31 May 2011 on the evaluation report from the Commission to the Council and the European Parliament on the Data retention Directive (Directive 2006/24/EC), e.g. paragraph 24.

([2]) The EDPS would like to recall the problems linked to the lack of a European definition of 'serious crime'. The EDPS indeed stressed that the evaluation report from the Commission on the Data Retention Directive shows that the choice of leaving the precise definition of what constitutes a 'serious crime' to the discretion of the Member States, has led to a wide variety of purposes for which the data have been used. The Commission has stated that 'most transposing Member States, in accordance with their legislation, allow the access and use of retained data for purposes going beyond those covered by the Directive, including preventing and combating crime generally and the risk of life and limb'. See Opinion of 31 May 2011 on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), §§24, 71 and 72.

([3]) According to Article 71.2 (d), competent authority under the proposed MiFID are allowed to require existing telephone and existing data traffic records held by investment firms where a reasonable suspicion of a breach of the proposed MIFIF exists.

([4]) See EDPS Opinion of 10 February 2012 on 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 (Recast) 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.

competent auhtority shall be notified without delay. The Commission will adopt the regulatory technical standards to determine appropriate arrangements and procedures referred to in the first paragraph and to determine the systems and notifications templates mentioned in the second paragraph (Article 11.3 last sentence).

36. As far as these systems will most probably involve personal data (e.g. monitoring of transactions made by persons referred to on insider's list), the EDPS would underline that these standards should be developed according to the principle of 'privacy by design', i.e. the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data ([1]). In addition, the EDPS recommends including a reference to the need to consult the EDPS in so far as these regulatory standards concern the processing of personal data.

2.5. **Exchange of information with third states**

37. The EPDS notes the reference to Directive 95/46/EC, particularly to Articles 25 or 26 and the specific safeguards mentioned in Article 23 of the proposed Regulation concerning the disclosure of personal data to third countries. Specifically, 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 are considered to represent appropriate safeguards in view of the risks concerned in such transfers.

2.6. **Publication of sanctions**

2.6.1. *Mandatory publication of sanctions*

38. Article 26.3 of the proposed Regulation obliges Member States to ensure that the competent authorities publish every administrative measure and sanction imposed for breaches of the proposed Regulation without undue delay, including at least information on the type and nature of the breach and the identity of persons responsible for it, unless such disclosure would seriously jeopardise the stability of financial markets.

39. 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. It would, furthermore, increase transparency, as market operators would be made aware that a breach has been committed by a particular person. 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.

40. The EDPS welcomes the reference in recital 35 to the Charter of Fundamental Rights and in particular the right to protection of personal data when adopting and publishing sanctions. However, he 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 the *Schecke* judgment ([2]). He takes the view that the purpose, necessity and proportionality of the measure are not sufficiently established and that, in any event, adequate safeguards should be provided for against the risks for the rights of the individuals should have been foreseen.

2.6.2. *Necessity and proportionality of the publication*

41. In the *Schecke* judgment, the Court of Justice annulled the provisions of a Council Regulation and a Commission Regulation providing for 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.

([1]) See EDPS Opinion of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union' (OJ C 181, 22.6.2011, p. 1), paragraphs 108 to 115.

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

42. After analysing that 'derogations and limitations in relation to the protection of personal data must apply only in as far as is strictly necessary', the Court went 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.

43. Article 26.3 of the proposed Regulation 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 ([1]).

44. 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 only refers to general positive impacts (i.e. deterrent effect of market abuse, contribution to investor protection, equal treatment of the issuers, improved enforcement) and merely mentions that 'publication of sanctions is of high importance to enhance transparency and maintain confidence in financial market' and that 'publication of imposed sanctions will contribute to the objective of deterrence and improves market integrity and investor protection' ([2]). 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.

45. Furthermore, the impact assessment report does not seem to take into account less intrusive methods, such as 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 26.1 (d) — 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. ([3]).

46. The impact assessment report does not explain why the publication on a case by case basis is not a sufficient option. It only mentions that the publication of imposed sanctions will 'contribute to the objective of eliminating options and discretions where possible by removing the current discretion Member States have not to require such publication' ([4]). In the EDPS view, the possibility to assess the case in light of the specific circumstances is 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. The assessment made in the impact assessment therefore does not dispel the doubts as to the necessity and proportionality of the measure.

2.6.3. *The need for adequate safeguards*

47. The proposed Regulation 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 a decision before a court and the presumption of innocence. Specific

([1]) 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).
([2]) See impact assessment p. 166.
([3]) I.e., in accordance with Article 27 of the proposed Regulation laying down the criteria for the determination of sanctions.
([4]) See impact assesment p. 167.

language ought to have been included in the text of Article 26.3 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 ([1]).

48. Secondly, the proposed Regulation 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 ([2]).

49. Thirdly, while the proposed Regulation 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 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 ([3]).

50. 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 ([4]). 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 ([5]).

2.6.4. *Conclusion*

51. 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 rights 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.

2.7. **Reporting of breaches**

52. Article 29 of the proposed Regulation requires Member States to put in place effective 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 ([6]).

([1]) 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.

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

([3]) 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

([4]) 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.

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

([6]) 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 whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (WP Opinion on whistleblowing). The Opinion can be found on the Article 29 WP webpage: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

53. The EDPS welcomes the fact that the proposed Regulation 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 EDPS is conscious of the fact that the proposed Regulation 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.

54. The EDPS highlights, as in the case of other Opinions ([1]), 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 ([2]). 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) ([3]). In view of the above, the EDPS recommends to add in letter b of Article 29.1 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'.

55. The EDPS is pleased to see that Article 29.1 (c) 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, 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.

3. **CONCLUSIONS**

56. The EDPS welcomes the attention specifically paid to data protection in the proposed Regulation.

57. The EDPS makes the following recommendations:

— Specify in Article 13 the purpose of the insider list;

— Introduce in Article 17.2 (e) concerning the power to enter private premises, the prior judicial authorisation as a general requirement;

— Introduce in Article 17.2 (f) 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;

([1]) 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

([2]) 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 3 February 2012, 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).

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

— Specify the categories of telephone and data traffic records held by a telecommunication operator and by an investment firms which competent authorities can require and to limit Article 17.2 (f) to data normally processed ('held') by telecommunications operators in the framework of Directive 2002/58/EC;

— Add in Article 29.1 (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';

— 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.

Done at Brussels, 10 February 2012.

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor