Opinion of the European Data Protection Supervisor

on the Commission proposals for a Directive amending Directive 2006/43/EC on statutory audit of annual accounts and consolidated accounts, and for a Regulation on specific requirements regarding statutory audit of public-interest entities

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Article 28(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 30 November 2011, the Commission adopted a proposal concerning amendments to Directive 2006/43/EC on statutory audits[3]. The amendments to Directive 2006/43/EC concern the approval and registration of auditors and audit firms, the principles regarding professional ethics, professional secrecy, independence and reporting as well as the associated supervision rules. On the same date, the Commission adopted a proposal for a Regulation on statutory audit of public-interest entities[4], which lays down the conditions for carrying out such audits (hereinafter 'the proposed Regulation'). These proposals were sent to the EDPS for consultation on 6 December 2011.

2. The EDPS welcomes the fact that he is consulted by the Commission and recommends that a reference to this Opinion is included in the preamble of the

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2011)778.
[4] COM(2011)779.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

Directive. A reference to the EDPS consultation has already been included in the preamble of the proposed Regulation.

3. In this Opinion, the EDPS addresses issues relating to Directive 2006/43/EC which go beyond what is covered by the proposed amendments. He emphasises the potential data protection implications of the Directive itself[5]. The analysis presented in this Opinion is directly relevant for the application of the existing legislation and for other pending and possible future proposals containing similar provisions, such as those discussed in the EDPS Opinions on the legislative package on the revision of the banking legislation, credit rating agencies, markets in financial instruments (MIFID/MIFIR) and market abuse[6]. Therefore, the EDPS recommends reading this Opinion in close conjunction with his Opinions of 10 February 2012 on the above mentioned initiatives.

1.2. Objectives and scope of the proposal

4. The Commission considers audit firms as contributing players to the financial crisis, and seeks to address the role auditors played in the crisis – or indeed the role they should have played. The Commission also states that robust audit is key to re-establishing trust and market confidence.

5. The Commission mentions that it is also important to stress that auditors are entrusted by law to conduct statutory audits of the financial statements of companies which enjoy limited liability and/or are authorised to provide services in the financial sector. This entrustment responds to the fulfilment of a societal role in offering an opinion on the truth and fairness of the financial statements of those companies.

6. Finally, according to the Commission, the financial crisis has highlighted weaknesses in the statutory audit especially with regard to Public-Interest Entities (PIE). These are entities which are of significant public interest because of their business, their size, their number of employees or their corporate status, or because they have a wide range of stakeholders.

7. In order to address these concerns, the Commission has published a proposal to amend Directive 2006/43/EC on statutory audits, which concerns the approval and registration of auditors and audit firms, the principles regarding professional ethics, professional secrecy, independence and reporting as well as the associated supervision rules. The Commission has also proposed a new Regulation on statutory audit of public-interest entities laying down the conditions for carrying out such audits.

8. The Commission proposes that Directive 2006/43/EC shall apply to situations not covered by the proposed Regulation. Therefore it is important to introduce a clear separation between the two legal texts. This means that the current provisions in Directive 2006/43/EC that only relate to the performance of a statutory audit on

[5] The EDPS was not consulted by the Commission on the proposal for a Directive 2006/43/EC on statutory audits; the Directive itself was adopted on 17 May 2006.
[6] EDPS Opinions of 10 February 2012, available at www.edps.europa.eu.

the annual and consolidated financial statements of the public-interest entities is moved to and, as appropriate, amended in the proposed Regulation.

1.3. Aim of the EDPS Opinion

9. The implementation and application of the legal framework for statutory audits may in certain cases affect the rights of individuals relating to the processing of their personal data. Directive 2006/43/EC in its current and amended form and the proposed Regulation contain provisions which may have data protection implications for the individuals concerned.

2. ANALYSIS OF THE PROPOSAL

2.1. Applicability of data protection legislation

10. The EDPS welcomes the attention specifically paid to data protection in the proposed Regulation. Recitals and provisions of the proposed Regulation mention the Charter of Fundamental Rights, Directive 95/46/EC and Regulation (EC) No 45/2001[7]. In particular, Article 56 of the proposed Regulation states that Member States shall apply Directive 95/46/EC to the processing of personal data under the proposed Regulation and that Regulation (EC) No 45/2001 shall apply to the processing of personal data carried out by the European Securities and Markets Authority (ESMA), the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) in the context of the proposed Regulation.

11. The EDPS much welcomes this type of overarching provision but suggests rephrasing the provision emphasising the full applicability of existing data protection legislation and replacing the multiple references in different articles of the proposed Regulation with one general provision referring to Directive 95/46/EC as well as Regulation (EC) No 45/2001. 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.

12. The EDPS recommends including a similar provision in Directive 2006/43/EC as well, as it is currently lacking.

2.2. Provisions regarding exchanges of information

2.2.1 Exchange of information between competent authorities

13. The current Directive and the proposed Regulation contain provisions allowing or requiring competent authorities to exchange information between them. In particular, Article 36 of Directive 2006/43/EC and Article 48 of the proposed Regulation state that competent authorities shall exchange information and cooperate in investigations related to the carrying-out of their duties under the legislative instruments.

[7] i.e. recitals 13, 14, 41, 42 and 47 and Articles 38, 56, 57 and 64.

14. It is evident that in some cases these exchanges of information will relate to identified or identifiable individuals and therefore constitute the processing of personal data under Article 2(b) of Directive 95/46/EC and Article 2(b) of Regulation (EC) No 45/2001.

15. The EDPS recognises the importance of ensuring a swift exchange of information between national competent authorities with a view to effectively supervising statutory auditors. However, a fair balance between the right to obtain and communicate information and the right to personal data protection must be sought. The risk is to be avoided in particular that the provisions allowing or requiring the exchange of information could be construed as a blanket authorisation to exchange all kinds of personal data.

16. A basic requirement of data protection law is that information must be processed for specified, explicit and legitimate purposes and that it may not be further processed in a way incompatible with those purposes. The data used to achieve the purposes should furthermore be adequate, relevant and not excessive in relation to these purposes[8].

17. As regards purpose limitation, it must be stressed that Directive 2006/43/EC and the proposed Regulation fail to specify the purposes of the system for exchange of information and, most importantly, the purposes for which the information held by competent authorities can be accessed by other competent authorities using their investigatory powers under Article 38 of the proposed Regulation.

18. Furthermore, Directive 2006/43/EC and the proposed Regulation fail to specify the kind of data that will be recorded, reported and accessed, including any personal data of identified or identifiable persons.

19. Finally, Article 6 of Directive 95/46/EC and Article 4 of Regulation (EC) 45/2001 require that personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The EDPS notes that the proposals do not lay down any concrete limitation of the period for the retention of the personal data potentially processed under Article 36 of Directive 2006/43/EC and Article 48 of the proposed Regulation. This is in contradiction with the requirements set out by data protection legislation, and may at least result in undue diversity in national implementation or practice.

20. On the basis of the foregoing, the EDPS urges the legislator to define the purposes for which personal data can be processed by the various entities concerned, to specify the kind of personal information that can be processed under Directive 2006/43/EC and the proposed Regulation and fix a precise, necessary and proportionate data retention period for the above processing.

[8] see Article 6 of Directive 95/46/EC and Article 4 of Regulation (EC) 45/2001.

2.2.2. Exchanges of information with third countries

21. The EDPS notes the reference to Chapter IV of Directive 95/46/EC in Article 13(1) of the proposed Regulation regarding the transfer of relevant documentation of audit work performed. Furthermore, the EDPS notes the references to compliance with Directive 95/46/EC and Regulation (EC) No 45/2001 in Article 57(1) of the proposed Regulation concerning Agreements on exchanges with third countries.

22. He also notes the reference to Chapter IV of Directive 95/46/EC in Article 47(1) of Directive 2006/43/EC regarding transfers of audit working papers or other documents held by statutory audit firms under certain conditions.

23. In line with his recommendations above[9] he would, however, advocate a more general reference in a specific Article of Directive 2006/43/EC and the proposed Regulation.

24. The EDPS welcomes the explicit reference to the existence of an adequate level of protection of personal data in the third country receiving the personal data in Directive 2006/43/EC, but recommends adding that in the absence of an adequate level of protection an assessment should take place on a case-by-case basis. He also recommends including a similar reference and the assessment on a case-by-case basis in the relevant provisions of the proposed Regulation.

2.3. Record keeping under the proposed Regulation

25. Article 30 of the proposed Regulation obliges audit firms to retain documents and information regarding client account records and audit files for at least 5 years. According to paragraph 2 of the same Article this period can be extended by Member States in accordance with national rules on personal data protection and judicial proceedings. If the records kept concern natural persons, this involves 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 databases.

26. Article 6(1)(e) of Directive 95/46/EC requires that personal data should not be kept for longer than is necessary for the purposes for which the data were collected or for which they are further processed. 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 purposes for which data are processed[10].

2.4. Power of the competent authorities to require records of telephone and data traffic

27. Article 38 of the proposed Regulation states that the competent authorities shall have all the investigatory powers that are necessary for the exercise of their functions, including the power to require records of telephone and data traffic

[9] see paragraphs 10 and 11 above.

[10] see EDPS Opinion of 10 February 2012 on markets in financial instruments (MIFID/MIFIR) (paragraph 16), available at www.edps.europa.eu

processed by statutory auditors and audit firms. The provision clearly implies that exchanges of personal data will take place under the proposed Regulation. It seems likely -or at least it cannot be excluded- that the records of telephone and data traffic concerned include personal data within the meaning of Directive 95/46/EC and Regulation (EC) No 45/2001 and, to the relevant extent, Directive 2002/58/EC (also known as 'the e-Privacy Directive'), i.e. data relating to the telephone and data traffic of identified or identifiable natural persons. In this 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[11].

28. Having said this, the EDPS welcomes that the proposed Regulation requires prior judicial authorisation in all cases in order for the competent authorities to request access to records of telephone and data traffic, a solution the EDPS has recommended for other proposals in the field of financial supervision[12].

29. 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 the 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. It is therefore essential in this perspective that the provisions are clear on 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 against the risk of abuse.

30. There is no definition of the notions of 'records of telephone and data traffic' in the proposed Regulation. Directive 2002/58/EC only refers to 'traffic data' but not to 'records of telephone and data traffic'[13]. 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 using the terminology already in place in the definition of 'traffic data' as well as making a reference to the relevant Article of Directive 2002/58/EC.

31. In the absence of said definition, the term 'records of telephone and data traffic' needs to be clarified. The provision might refer to records of telephone and data traffic, which auditors and audit firms are obliged to retain in the course of their activities. However, the proposed Regulation does not specify if and what records

[11] see EDPS Opinions of 10 February 2012 on credit rating agencies (paragraph 23), markets in financial instruments (MIFID/MIFIR) (paragraph 46) and market abuse (paragraphs 26), available at www.edps.europa.eu.

[12] see EDPS Opinions of 10 February 2012 on credit rating agencies (paragraph 24), markets in financial instruments (MIFID/MIFIR) (paragraph 47) and market abuse (paragraph 27), available at www.edps.europa.eu.

[13] Article 2(1)(b) of 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.

of telephone and data traffic must be collected by audit firms. Therefore, it is essential to define precisely the categories of telephone and data traffic that have to be retained and can be required by competent authorities. In line with the principle of proportionality, such data must be adequate, relevant and not excessive in relation to the supervisory purposes for which they are processed.

32. According to the EDPS, the circumstances and the conditions for using the investigatory powers of the competent authorities should be more clearly defined. Article 38(1)(d) of the proposed Regulation does not indicate the circumstances and the conditions under which access to records of telephone and data traffic can be required. Nor does it provide for important procedural guarantees or safeguards against the risk of abuses. The EDPS therefore recommends limiting access to records of telephone and data traffic to specifically identified and serious violations of the proposed Regulation and in cases where a reasonable suspicion (which should be supported by concrete initial evidence) exists that a breach has been committed[14].

33. 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 a court of law.

2.5. Mandatory publication of sanctions

34. The proposed Regulation in Article 62 empowers competent authorities to impose sanctions on the individuals responsible for a breach of the proposed Regulation as laid down in its Annex. The Annex refers to breaches committed by natural persons such as auditors and key audit partners. Article 64 obliges competent authorities to publish every sanction imposed for a breach. The obligation to publish sanctions 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. Recital 41 of the proposed Regulation also states that the sanctioning powers of competent authorities should be enhanced and that the competent authorities should be transparent about the measures they apply. Also, Article 30(3) of Directive 2006/43/EC states that Member States shall provide that penalties imposed on statutory auditors are appropriately disclosed to the public.

35. The EDPS notes that both Article 64 and Recital 41 of the proposed Regulation state that the publication of sanctions shall respect fundamental rights as laid down in the EU Charter of Fundamental Rights, in particular the right to protection of personal data.

36. The impact assessment refers to the fact that the obligation to publish sanctions may have a negative impact on the fundamental right to protection of personal data with regard to the individuals concerned but that publication of sanctions is an important element in ensuring that sanctions have a dissuasive effect on the

[14] see EDPS Opinions of 10 February 2012 on credit rating agencies (paragraph 35) and market abuse (paragraph 33), available at www.edps.europa.eu.

author of the violation and is necessary to ensure that sanctions have a dissuasive effect on the general public. It furthermore mentions that the 'publication of sanctions is considered to be one of the most deterrent tools to prevent violations, particularly because of the reputational damage that the author of the violation will incur'. 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. The purpose of the publication of sanctions should be mentioned in the Articles concerned both in Directive 2006/43/EC and in the proposed Regulation.

37. 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, taking account of the relevant circumstances, such the gravity of the breach, the degree of personal responsibility, recidivism, losses for third parties, etc.

38. 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'. 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. An explanation of the necessity and proportionality of the mandatory publication of sanctions should be included in the recitals of Directive 2006/43/EC and the proposed Regulation.

39. In view of the above, the EDPS 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 individual. The EDPS recommends that the purpose of the publication of sanctions should be mentioned in the Articles concerned both in Directive 2006/43/EC and in the proposed Regulation and that an explanation of the necessity and proportionality of the publication should be included in the recitals of Directive 2006/43/EC and the proposed Regulation. He also recommends that publication should be decided on a case-by-case basis and that a possibility to publish less information than currently required should be provided.

2.6. Reporting of breaches

40. Article 66 of the proposed Regulation deals with mechanisms for the reporting of 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. The EDPS welcomes the fact that the proposed provision contains certain 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 recommend including some further specifications.

41. 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[15]. 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. Furthermore, the preference for identified and confidential reports compared to 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 should be respected.

42. The procedures for the receipt of the report and their follow-up referred to in Article 66(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. Specific wording should be added to this effect. In this respect, the EDPS recommends using the wording of the Commission proposal for a Regulation on insider dealing and market manipulation. Article 29(d)[16] of this proposal specifically requires 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'[17].

43. Moreover, the EDPS highlights 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[18]. 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. 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.

---

[15] see 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), available at: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

[16] COM(2011)651.

[17] see EDPS Opinions of 10 February 2012 on the legislative package on the revision of the banking legislation (paragraph 35), markets in financial instruments (MIFID/MIFIR) (paragraph 68) and market abuse (paragraphs 52-53), available at www.edps.europa.eu.

[18] see EDPS Opinion of 15 April 2011 on the Financial rules applicable to the annual budget of the Union, OJ C 215, 21.07.2011, p 13-18.

44. As to judicial procedures: 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). In view of the above, the EDPS recommends adding in letter b) of Article 66(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'.

45. Finally, as regards Article 66(1)(c), 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.

3. CONCLUSIONS

46. The EDPS welcomes the attention specifically paid to data protection in the proposed Regulation, but identified some scope for further improvement.

47. The EDPS makes the following recommendations:

- rephrasing Article 56 of the proposed Regulation and inserting a provision in Directive 2006/43/EC emphasising the full applicability of existing data protection legislation and replacing the multiple references in different articles of the proposed Regulation with one general provision referring to Directive 95/46/EC as well as Regulation (EC) No 45/2001. 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;

- specifying the kind of personal information that can be processed under Directive 2006/43/EC and the proposed Regulation, to define the purposes for which personal data can be processed by the competent authorities concerned and fix a precise, necessary and proportionate data retention period for the above processing;

- in view of the risks concerned regarding transfers of data to third countries, the EDPS recommends adding to Article 47 of Directive 2006/43/EC that in the absence of an adequate level of protection an assessment should take place on a case-by-case basis. He also recommends including a similar reference and the assessment on a case-by-case basis in the relevant provisions of the proposed Regulation;

- replacing the minimum retention period of 5 years in Article 30 of the proposed Regulation with a maximum retention period. The chosen period should be necessary and proportionate for the purpose for which data are processed;

- mentioning the purpose of the publication of sanctions in the Articles concerned in Directive 2006/43/EC and in the proposed Regulation and explaining the necessity and proportionality of the publication in the recitals of both Directive 2006/43/EC and the proposed Regulation. He also recommends that publication should be decided on a case-by-case basis and that a possibility to publish less information than currently required should be catered for;

- providing for adequate safeguards regarding mandatory publication of sanctions 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;

- adding a provision in Article 66(1) of the proposed Regulation 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';

- removing the wording 'the principles laid down' from Article 66(1)(c) of the proposed Regulation.

Done in Brussels, 13 April 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor