I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Commission proposals for a Directive on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and for a Regulation on prudential requirements for credit institutions and investment firms

(2012/C 175/01)

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 July 2011, the Commission adopted two proposals concerning the revision of the banking legislation. The first proposal concerns a Directive on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (the 'proposed Directive') [4]. The second proposal concerns a Regulation on prudential requirements for credit institutions and investment firms (the proposed 'Regulation') [5]. These proposals were sent to the EDPS for consultation on the same day. On 18 November 2011, the Council of the European Union consulted the EDPS on the proposed Directive.

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 the fact that he is consulted by the Commission and the Council and recommends that a reference to the present Opinion is included in the preamble of the instruments adopted.

[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] COM(2011) 453.
[5] COM(2011) 452.

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

5. The proposed legislation comprises two legal instruments: a Directive on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms and a Regulation on prudential requirements for credit institutions and investment firms. The policy objectives of the proposed revision are in short to ensure the smooth operation of the banking sector and restore confidence by the operators and the public. The proposed instruments will replace Directive 2006/48/EC and Directive 2006/49/EC, which will be consequently repealed.

6. The main new elements of the proposed Directive are provisions on sanctions, effective corporate governance and provisions preventing overreliance on external credit ratings. In particular, the proposed Directive aims to introduce an effective, proportionate sanctioning regime, appropriate personal scope of administrative sanctions, publication of sanctions and mechanisms encouraging the reporting of violations. Moreover, it aims at strengthening the legislative framework regarding corporate governance and to reduce over-reliance on external ratings ([6]).

7. The proposed Regulation complements the proposed Directive by establishing uniform and directly applicable prudential requirements for credit institutions and investment firms. As stated in the explanatory memorandum, the overarching goal of the initiative is to ensure that the effectiveness of the institutional capital regulation in the EU is strengthened and its adverse impact on the financial system is contained ([7]).

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

8. While most of the provisions of the proposed instruments relate to the pursuit of the activities of credit institutions, the implementation and application of the legal framework may in certain cases affect the rights of individuals relating to the processing of their personal data.

9. Several provisions of the proposed Directive allow for the exchange of information between the authorities of the Member States and, possibly, third countries ([8]). This information may well relate to individuals, such as the members of the management of the credit institutions, their employees and shareholders. Furthermore, under the proposed Directive competent authorities may impose sanctions directly on individuals and are obliged to publish the sanctions inflicted, including the identity of the individuals responsible ([9]). In order to facilitate the detection of violations, the proposal introduces the obligation for the competent authorities to put in place mechanisms encouraging the reporting of breaches ([10]). Moreover, the proposed Regulation obliges credit institutions and investment firms to disclose information relating to their remuneration policies, including the amounts paid segregated per categories of staff and per pay-bands ([11]). All these provisions may have data protection implications for the individuals concerned.

10. In light of the above, the present Opinion will focus on the following aspects of the package relating to privacy and data protection: 1. applicability of data protection legislation; 2. data transfers to third countries; 3. professional secrecy and use of confidential information; 4. mandatory publication of sanctions; 5. mechanisms for the reporting of breaches; 6. disclosure requirements concerning remuneration policies.

2. **ANALYSIS OF THE PROPOSALS**

2.1. **Applicability of data protection legislation**

11. Recital 74 of the proposed Directive contains a reference to the full applicability of data protection legislation. However, a reference to the applicable data protection legislation should be inserted in a substantive article of the proposals. 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

([6]) Explanatory memorandum of the proposed Directive, pp. 2-3.
([7]) Explanatory memorandum of the proposed Regulation, pp. 2-3.
([8]) See, in particular, Articles 24, 48 and 51 of the proposed Directive.
([9]) Articles 65(2) and 68 of the proposed Directive.
([10]) Article 70 of the proposed Directive.
([11]) Article 435 of the proposed Regulation.

dealing and market manipulation ([12]), 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.

12. This is particularly relevant, for example, in relation to the various provisions concerning exchanges of personal information. These provisions are perfectly legitimate but need to be applied in a way which is consistent with data protection legislation. The risk is to be avoided in particular that they could be construed as a blanket authorisation to exchange all kind of personal data. A reference to data protection legislation, also in the substantive provisions, would significantly reduce such risk.

13. 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 ([13]), subject to the suggestions he made on this proposal ([14]), 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.

2.2. **Transfers to third countries**

14. Article 48 of the proposed Directive provides that the Commission may submit proposals to the Council for the negotiation of agreements with third countries seeking to ensure, among others, that the competent authorities of third countries are able to obtain the information necessary for the supervision of parent undertakings situated in their territories and having a subsidiary in one or more Member States.

15. To the extent that this information contains personal data, Directive 95/46/EC and Regulation (EC) No 45/2001 are fully applicable with regard to transfers of data to third countries. The EDPS suggests clarifying in Article 48 that in these cases such agreements must comply with the conditions for transfers of personal data to third countries laid down in Chapter IV of Directive 95/46/EC and in Regulation (EC) No 45/2001. The same should be foreseen with regard to Article 56 concerning cooperation with competent authorities of third countries agreements entered into by Member States and EBA.

16. In addition to this, in view of the risks concerned in such transfers, the EDPS recommends adding specific safeguards as has been done in Article 23 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation. In the EDPS Opinion on this proposal he welcomes the use of such a provision containing appropriate safeguards, such as case-by-case assessment, ensuring the necessity of the transfer and the existence of an adequate level of protection of personal data in the third country receiving the personal data.

2.3. **Professional secrecy and use of confidential information**

17. Article 54 of the proposed Directive states that staff members of the competent authorities must respect the obligation of professional secrecy. The second subparagraph of Article 54 prohibits the disclosure of confidential information, 'except in summary or collective form, such that individual credit institutions cannot be identified […].' As it is formulated, it is not clear whether the prohibition also covers disclosure of personal information.

18. The EDPS recommends extending the prohibition of disclosing confidential information contained in the second-subparagraph of Article 54(1) to cases where individuals are identifiable (i.e. not only 'individual credit institutions'). In other words, the provision should be reformulated so as to prohibit the disclosure of confidential information, 'except in summary or collective form, such that individual credit institutions and individuals cannot be identified' (emphasis added).

([12]) Commission proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, COM(2011) 651.
([13]) See footnote 12.
([14]) See Opinion 10 February 2012 on the Commission's 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, COM(2011) 651.

2.4. **Provisions concerning publication of sanctions**

2.4.1. *Mandatory publication of sanctions*

19. One of the main objectives of the proposed package is to reinforce and approximate Member States' legal framework concerning administrative sanctions and measures. The proposed Directive provides for the power of the competent authorities to impose sanctions, not only on credit institutions, but also on the individuals materially responsible for the breach ([15]). Article 68 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.

20. 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 ([16]). 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.

21. The EDPS is not convinced that the mandatory publication of sanctions, as it is currently formulated, meet the requirements of data protection law as clarified by the Court of Justice in the the *Schecke* judgment ([17]). He takes the view that the purpose, necessity and proportionality of the measure are not sufficiently established and that, in any event, adequate safeguards for the rights of the individuals should have been foreseen.

2.4.2. *Necessity and proportionality of the publication*

22. 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.

23. 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 in that case 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.

24. Article 68 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 when 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 ([18]).

25. 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 addressees and is necessary to ensure that sanctions have a dissuasive effect on the general public'. However, the report does not consider whether less intrusive

([15]) The personal scope of the sanctions is clarified in Article 65 of the proposed Directive establishing that Member States shall ensure that where obligations apply to institutions, financial holding companies and mixed-activity holding company, in case of a breach sanctions can be applied to the member of the management body, and to any other individuals who under national law are responsible for the breach.

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

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

([18]) 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).

methods might have guaranteed the same result in terms of deterrence without interfering with the privacy rights of the individuals concerned. It does not explain, in particular why financial penalties or other types of sanctions not affecting privacy would not be sufficient.

26. Furthermore, the impact assessment report does not seem to sufficiently take into account less intrusive methods of publishing the information, such as limiting the publication to the identity of credit institutions or even considering the need for publication 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 publication is itself a sanction under Article 67(2)(a) and that Article 69 provides that when determining the application of sanctions the competent authorities should take account of the relevant circumstances (i.e. case by case assessment), such as the gravity of the breach, the degree of personal responsibility, recidivism, losses for third parties, etc. The obligatory publication of sanctions in all cases under Article 68 is inconsistent with the sanctioning regime set out in Articles 67 and 69.

27. The impact assessment report dedicates only a few paragraphs to explain why the publication on a case by case basis is not a sufficient option. It states that leaving to competent authorities to decide 'if the publication is appropriate' would reduce the deterrent effect of the publication ([19]). However, in the EDPS view, it is exactly this aspect -i.e. the possibility to assess the case in light of the specific circumstances- which makes this solution a 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.

2.4.3. *The need for adequate safeguards*

28. 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 68 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 ([20]).

29. 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 ([21]).

30. 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 ([22]).

([19]) See pp. 44-45.

([20]) 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.

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

([22]) 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. 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 ([23]). 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 ([24]).

2.4.4. *Conclusions on publication*

32. 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 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 appropriate period of time.

2.5. **Reporting of breaches**

33. Article 70 of the proposed Directive deals with mechanisms for reporting violations, 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 ([25]). The EDPS welcomes the fact that the Proposal 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 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.

34. The EDPS highlights, as in the case of other Opinions ([26]), 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 processed under conditions of confidentiality, in particular vis-à-vis the person about whom an alleged wrongdoing is being reported ([27]). 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) ([28]). In view of the above, the EDPS recommends to add in letter b of Article 70 the following provision:

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

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

([25]) 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

([26]) See for instance, the EDPS Opinion on financial rules applicable to the annual budget of the Union of 15 April 2011 (OJ C 215, 21.7.2011, p. 13) and the Opinion on investigations conducted by OLAF of 1 June 2011 (OJ C 279, 23.9.2011, p. 11).

([27]) 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).

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

'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'.

35. 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 ([29]). The procedures for the receipt of the report and their follow-up referred to in Article 70(2)(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 ([30]). 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'.

36. Finally, as regards letter (c) of paragraph 2, the EDPS is pleased to see that this provision requires Member States to ensure the protection of personal data of both the 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 whistleblowing. 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**

37. 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 EBA within the framework of this Regulation, EBA shall comply with the provisions of Regulation (EC) No 45/2001';

— amend the second subparagraph of Article 54(1) so as to permit disclosure of confidential information only in summary or collective form, 'such that individual credit institutions and individuals cannot be identified' (emphasis added);

— clarify in Article 48 and Article 56 that agreements with third countries or third country authorities providing for the transfer of personal data must comply with the conditions for transfers of personal data to third countries laid down in Chapter IV of Directive 95/46/EC and in Regulation (EC) No 45/2001 and introduce also in the proposed Directive provision similar to Article 23 of the proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation ([31]);

([29]) 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 pp. 8 and 9) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-04-23_Guidelines_inquiries_EN.pdf

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

([31]) See footnote 12.

— 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;

— with regard to Article 70 1. add in letter (b) of Article 70 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'; 2. 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'; 3. remove 'the principles laid down' from letter (c) of the provision.

Done at Brussels, 10 February 2012.

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor