Opinion of the European Data Protection Supervisor on the Commission proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 1060/2009 on credit rating agencies

(2012/C 139/02)

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 four EDPS' opinions relating to the financial sector, all adopted on the same day.

2. On 15 November 2011, the Commission adopted a proposal concerning amendments to the Regulation (EC) No 1060/2009 on credit rating agencies (hereinafter 'CRA Regulation') [3]. This proposal was sent to the EDPS for consultation on 18 November 2011.

3. 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 instrument adopted.

4. The EDPS regrets, however, that he was neither formally consulted by the Commission during the preparation of the original CRA Regulation that entered into force on 7 December 2010, nor regarding the recent amendments to the said Regulation [4].

5. In this Opinion, the EDPS therefore finds it appropriate and useful to address issues regarding the CRA Regulation already in place. Firstly, he emphasises the potential data protection implications of the CRA Regulation itself. Secondly, 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 discussed in the EDPS Opinions on the legislative package on the revision of the banking legislation, markets in financial instruments (MIFID/MIFIR) and market abuse.

1.2. Objectives and scope of the proposal and the current Regulation

6. The Commission considers credit rating agencies (CRAs) to be important financial market participants, which need to be subject to an appropriate legal framework. The first CRA Regulation entered into force on 7 December 2010. It requires CRAs to comply with rigorous rules of conduct in order to mitigate possible conflicts of interest, ensure high quality and sufficient transparency of ratings and the rating process. Existing CRAs had to apply for registration and to comply with the requirements of the Regulation by 7 September 2010.

7. Amendments to the CRA Regulation (Regulation (EU) No 513/2011) entered into force on 1 June 2011, entrusting ESMA with exclusive supervisory powers over CRAs registered in the EU in order to centralise and simplify their registration and supervision at European level.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2011) 747.
[4] Regulation (EU) No 513/2011, which entered into force on 1 June 2011.

8. The current proposed legislation constitutes amendments to the CRA Regulation but does not replace it. The main policy objective of the proposed revision is to address a number of issues related to CRAs and the use of ratings that have not been sufficiently addressed in the existing CRA Regulation.

1.3. **Aim of the EDPS Opinion**

9. While most of the provisions of the CRA Regulation relate to the pursuit of the activities of CRAs and the supervision of their activities, 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.

10. The CRA Regulation allows for the exchange of information between ESMA, competent authorities, sectoral competent authorities and, possibly, third countries ([5]). This information may well relate to individuals, such as persons involved in credit rating activities and persons otherwise closely and substantially related and connected to CRAs or credit rating activities. These provisions may have data protection implications for the individuals concerned.

11. In light of the above, this Opinion will focus on the following aspects of the CRA Regulation relating to privacy and data protection: 1. applicability of data protection legislation; 2. transfers of data to third countries; 3. access to records of telephone and data traffic; and 4. disclosure requirements regarding structured finance instruments and periodic penalty payments.

2. **ANALYSIS OF THE PROPOSAL**

2.1. **Applicability of data protection legislation** ([6])

12. Several recitals ([7]) of the CRA Regulation mention the Charter of Fundamental Rights, Directive 95/46/EC and Regulation (EC) No 45/2001. However, a reference to the applicable data protection legislation should be inserted in a substantive article of the CRA Regulation.

13. A good example of such a substantive provision can be found in Article 22 of the proposal for a regulation of the European Parliament and of the Council on insider dealing and market manipulation ([8]), which explicitly provides as a general rule that Directive 95/46/EC and Regulation (EC) No 45/2001 apply to the processing of personal data within the framework of the proposal. The EDPS today issued an Opinion on this proposal where he very much welcomes this type of overarching provision. However, the EDPS suggests that the reference to Directive 95/46/EC be clarified by specifying that the provisions will apply in accordance with the national rules which implement Directive 95/46/EC.

14. This is 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 ([9]).

([5]) See, in particular, Articles 23 and 27 of the CRA Regulation.
([6]) See also recent EDPS Opinions on the legislative package on the revision of the banking legislation (Section 2.1), markets in financial instruments (MIFID/MIFIR) (Section 2.1) and market abuse (Section 2.1).
([7]) See recitals 8, 33 and 34 of the CRA Regulation.
([8]) COM(2011) 651.
([9]) The CRA Regulation contains provisions allowing or requiring competent authorities and sectoral competent authorities to exchange information between them or with ESMA. In particular, Article 27 of the Regulation requires ESMA, sectoral competent authorities and competent authorities to provide each other with the information required for the purposes of carrying out their duties under the Regulation. Also, Article 23c empowers ESMA to conduct investigations of persons involved in credit rating activities and persons otherwise closely and substantially related and connected to CRAs or credit rating activities. According to Article 23b, these natural persons may also be requested to provide ESMA with all information deemed necessary. These provisions clearly imply that exchanges of personal data will take place under the CRA Regulation.

15. 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 ([10]), subject to the suggestions he made on this proposal ([11]), 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. **Exchanges of information with third countries** ([12])

16. The EPDS notes the reference to Regulation (EC) No 45/2001 in Article 34.3 of the CRA Regulation regarding the transfer of personal data to third countries.

17. However, 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, the assurance of 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. **Power of ESMA to request records of telephone and data traffic** ([13])

2.3.1. *Judicial authorisation*

18. Article 23c(1)(e) provides that in order to carry out its duties under this Regulation, ESMA may conduct all necessary investigations. To that end, its officials and other persons authorised by ESMA shall be empowered to request records of telephone and data traffic. Because of its broad wording, the provision raises several doubts concerning its material and personal scope. The CRA Regulation furthermore requires prior judicial authorisation in order for ESMA to request access to records of telephone and data traffic in case it is required according to national rules ([14]).

19. There is no definition of the notions of 'records of telephone and data traffic' in the proposed regulation. Directive 2002/58/EC (now called, as amended by Directive 2009/136/EC, 'the e-Privacy Directive') only refers to 'traffic data' but not to 'records of telephone and data traffic'. 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.

20. Data relating to use of electronic communication means may convey a wide range of personal information, such as the identity of the persons making and receiving the call, the time and duration of the call, the network used, the geographic location of the user in case of portable devices, etc. Some traffic data relating to Internet and e-mail use (for example, the list of websites visited) may in addition reveal important details of the content of the communication. Furthermore, processing of traffic data conflicts with the secrecy of correspondence. In view of this, Directive 2002/58/EC has established the principle that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication ([15]). According to

([10]) Commission proposal for a regulation of the European Parliament and of the Council on insider dealing and market manipulation, COM(2011) 651.
([11]) See the EDPS Opinion of 10 February 2012 on the proposal for a regulation of the European Parliament and of the Council on insider dealing and market manipulation, COM(2011) 651.
([12]) See also recent EDPS Opinions on the legislative package on the revision of the banking legislation (Section 2.2), markets in financial instruments (MIFID/MIFIR) (Section 2.8) and market abuse (Section 2.5).
([13]) See also recent EDPS Opinions on markets in financial instruments (MIFID/MIFIR) (Section 2.3) and market abuse (Section 2.3.2).
([14]) Article 23c(5).
([15]) See Article 6(1) of Directive 2002/58/EC (OJ L 201, 31.7.2002, p. 37).

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 ([16]).

21. The EDPS acknowledges that the aims pursued by the Commission in the CRA Regulation are legitimate. He understands the need for initiatives aiming at strengthening supervision of financial markets in order to preserve their soundness and better protect investors and economy at large. However, investigatory powers directly relating to traffic data, given their potentially intrusive nature, have to comply with the requirements of necessity and proportionality, i.e. they have to be limited to what is appropriate to achieve the objective pursued and not go beyond what is necessary to achieve it ([17]). 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.

22. Article 23c empowers ESMA to conduct investigations of persons involved in credit rating activities and persons otherwise closely and substantially related and connected to CRAs or credit rating activities. According to Article 23b, these natural persons may also be requested to provide ESMA with all information deemed necessary.

23. These provisions clearly imply that exchanges of personal data will take place under the CRA 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, *i.e.* data relating to the telephone and data traffic of identified or identifiable natural persons ([18]). 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.

24. The EDPS notes that Article 23c(5) makes judicial authorisation obligatory whenever such authorisation is required by national law. However, the EDPS considers that a general requirement for prior judicial authorisation in all cases — regardless of whether national law requires so — would be justified in view of the potential intrusiveness of the power at stake and the choice of a regulation as the appropriate legal instrument. 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.

25. As stated above under Section 2.1, the power for supervisory authorities to require access to records of telephone and data traffic is not new in European legislation as it is already foreseen in various existing directives and regulations concerning the financial sector. In particular, the Market Abuse Directive ([19]), the MiFID Directive ([20]), and the UCITS Directive ([21]) all contain similarly drafted provisions. The same

([16]) 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 (…)'.

([17]) 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.

([18]) Normally, the employees to whom the telephone and data traffic can be imputed as well as recipients and other users concerned.

([19]) 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).

([20]) Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ L 145, 30.4.2004, p. 1).

([21]) Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (OJ L 302, 17.11.2009, p. 32).

is true for a number of recent proposals adopted by the Commission, namely the proposals for a directive on alternative investment fund managers ([22]), a regulation on short selling and certain aspects of credit default swaps ([23]) and a regulation on integrity and transparency of energy markets ([24]).

26. As regards these existing and proposed legislative instruments, a distinction should be made between investigatory powers granted to national authorities and the granting of such powers to EU authorities. Several instruments oblige Member States to grant the power to require telephone and data traffic records to national authorities in conformity with national law ([25]). As a consequence, the actual execution of this obligation is necessarily subject to the national law including the one implementing Directives 95/46/EC and 2002/58/EC and other national laws which contain further procedural safeguards for national supervisory and investigatory authorities.

27. No such condition is contained in the CRA Regulation or the other legislative instruments which grant the power to require telephone and data traffic records directly to EU authorities. As a consequence, in these cases there is an even stronger requirement to clarify in the legislative instrument itself, the personal and material scope of this power and the circumstances in which and the conditions under which it can be used and to ensure that adequate safeguards against abuse are in place.

28. Article 23c(1)(e) of the Regulation empowers ESMA to request records of telephone and data traffic. As will be further explained below, the scope of the provision and in particular the exact meaning of 'records of telephone and data traffic' is not clear.

2.3.2. *The definition of 'records of telephone and data traffic'*

29. The definition of 'records of telephone and data traffic' is not entirely clear and thus needs to be clarified. The provision might refer to records of telephone and data traffic, which CRAs are obliged to retain in the course of their activities. However, the Regulation does not specify if and what records of telephone and data traffic must be collected by CRAs ([26]). Therefore, should the provision refer to records held by CRAs, it is essential to define precisely the categories of telephone and data traffic that have to be retained and can be required by ESMA. 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 ([27]).

30. More precision is needed particularly in this case, in consideration of the heavy fines and periodic penalty payments that CRAs and other persons (including natural persons as regards periodic penalty payments) concerned might incur for a breach of the Regulation (cf. Article 36a and Article 36b).

31. It should also be noted that the abovementioned Article 37 delegates to the Commission the power to adopt amendments allowing the Commission to amend annexes to the Regulation, which contain the details of record-keeping requirements imposed on Credit rating agencies, and thus, indirectly, the

([22]) Proposal of 30 April 2009 for a directive of the European Parliament and of the Council on alternative investment fund managers and amending Directives 2004/39/EC and 2009/65/EC, COM(2009) 207.

([23]) Proposal of 15 September 2010 for a regulation of the European Parliament and of the Council on short selling and certain aspects of credit default swaps, COM(2010) 482.

([24]) Regulation of the European Parliament and of the Council on energy market integrity and transparency, COM(2010) 726.

([25]) See for instance Article 12(2) of the Market Abuse Directive mentioned in footnote 20. See also Article 50 of the MiFID Directive, mentioned in footnote 21.

([26]) The expression 'records of telephone and data traffic' may potentially include a wide variety of information, including the duration, time or volume of a communication, the protocol used, the location of the terminal equipment of the sender or recipient, the network on which the communication originates or terminates, the beginning, end or duration of a connection or even the list of websites visited and the content of the communications themselves in case they are recorded. To the extent that they relate to identified or identifiable natural persons, all this information constitutes personal data.

([27]) See Article 6(1)(c) of Directive 95/46/EC and Article 4(1)(c) of Regulation (EC) No 45/2001. It should also be considered whether specific safeguards can be devised to avoid that data concerning genuinely private use are captured and processed.

power granted by ESMA to access records of telephone and data traffic. Article 290 of the TFEU provides that a legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend *non-essential elements* of the legislative act. According to the EDPS, the exact perimeter of the power to access traffic data cannot be considered a non-essential element of the Regulation. The material scope thereof should therefore be specified directly in the text of the Regulation and not deferred to future delegated acts.

32. The EDPS understands that the aim of Article 23c(1)(e) is not to allow ESMA to gain access to traffic data directly from telecom providers. This seems to be the logical conclusion particularly in consideration of the fact that the Regulation does not refer at all to data held by telecom providers or to the requirements set out by the e-Privacy Directive as mentioned in paragraph 36 above ([28]). Therefore, for the sake of clarity, he recommends making such conclusion more explicit in Article 23c of the CRA Regulation by specifically excluding traffic data held by telecom providers.

33. Should, however, a right to access to traffic data directly from telecom providers be envisaged, the EDPS has serious doubts about the necessity and proportionality of such a right and therefore recommends that such a right be explicitly excluded.

2.3.3. *Access to personal data*

34. Article 23c(1)(e) does not indicate the circumstances in which and the conditions under which access can be required. Neither does it provide for important procedural guarantees or safeguards against the risk of abuses. In the following paragraphs, the EDPS will make some concrete suggestions in this direction.

35. Article 23c(1) states that ESMA may require access to records of telephone and data traffic in order to carry out the duties under the CRA Regulation. According to the EDPS, the circumstances and the conditions for using such power should be more clearly defined. The EDPS 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. Such limitation is also particularly important with a view to avoiding the access power being used for the purpose of phishing operations or data mining or for different purposes.

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

2.4. **Provisions concerning disclosure of information**

2.4.1. *Information concerning structured finance instruments*

37. In the current proposal for amendments to the CRA Regulation ([29]), the proposed Article 8a regarding information on structured finance instruments states that the issuer, the originator and the sponsor of a structured finance instrument shall disclose to the public information on the credit quality and performance of the individual underlying assets of the structured finance instrument, the structure of the securitisation transaction, the cash flows and any collateral supporting a securitisation exposure as well as any information that is necessary to conduct comprehensive and well informed stress tests on

([28]) As said, the e-Privacy Directive establishes the general 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. Such data can be further processed only for the purpose of billing and interconnection payments and up to the end of the period during which the bill may lawfully be challenged or payment pursued. Any derogation to this principle must be necessary, appropriate and proportionate within a democratic society for specific public order purposes (i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems).

([29]) COM(2011) 747.

the cash flows and collateral values supporting the underlying exposures. The obligation to disclose information shall not extend to the provision of such information that would breach statutory provisions governing the protection of confidentiality of information sources or the processing of personal data.

38. This Article is aimed at the issuer, the originator and the sponsor of a structured finance instrument. The EDPS welcomes that, in the current proposal for amendments to the CRA Regulation, the proposed Article 8a introduces that the obligation to disclose information to the public shall not extend to the provision of such information that would breach statutory provisions governing the protection of confidentiality of information sources or the processing of personal data.

39. This way of emphasising the safeguards offered by laws governing the processing of personal data is in the opinion of the EDPS a step in the right direction, but in line with recommendations made above, a clear and explicit reference in a substantive Article of the CRA Regulation to the national rules implementing Directive 95/46/EC should be made.

2.4.2. *Information concerning periodic penalty payments* ([30])

40. Article 36d of the CRA Regulation states that ESMA shall disclose to the public every periodic penalty payment that has been imposed unless such disclosure to the public would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

41. According to Article 36b and Article 23b(1), persons involved in credit rating activities and persons otherwise closely and substantially related or connected to CRAs or credit rating activities can be subject to periodic penalty payments.

42. The CRA Regulation thus empowers ESMA to impose sanctions, not only on credit institutions, but also on the individuals materially responsible for the breach. In the same vein, Article 36d obliges ESMA to publish every periodic penalty payment imposed for a breach of the proposed regulation.

43. 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. 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.

44. The EDPS is not convinced that the mandatory publication of sanctions, as it is currently drafted, meets the requirements of data protection law as clarified by the Court of Justice in the *Schecke* judgment ([31]). 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.

2.4.3. *Necessity and proportionality of the mandatory publication of sanctions*

45. 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.

([30]) See also recent EDPS Opinions on the legislative package on the revision of the banking legislation (Section 2.4), markets in financial instruments (MIFID/MIFIR) (Section 2.5) and market abuse (Section 2.6).

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

46. 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.

47. Article 36d of the CRA 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 ([32]).

48. The EDPS is therefore under the impression that the purpose, and consequently the necessity, of this measure is not clearly established. The recitals of the CRA Regulation are silent on these issues. If the general purpose is increasing deterrence, it seems that the Commission should have explained, for instance, why heavier financial penalties (or other sanctions not amounting to naming and shaming) would not have been sufficient.

49. Furthermore, less intrusive methods should have been considered, such as publication limited to CRA's or publication to be decided on a case-by-case basis. In particular the latter option would seem to be *prima facie* a more proportionate solution.

50. However, in the EDPS view, the possibility to assess the case in light of the specific circumstances makes this solution more proportionate and therefore a preferred option compared to mandatory publication in all cases. This discretion would, for example, enable ESMA 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.

2.4.4. *The question of adequate safeguards*

51. The CRA 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 persons concerned to appeal and the presumption of innocence. Specific language ought to have been included in the text of Article 36d in this respect, so as to oblige ESMA 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 ([33]).

52. Secondly, the CRA Regulation should ensure that the rights of the data subjects are respected in a proactive manner. The EDPS appreciates the fact that the CRA Regulation 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 imposing a periodic penalty payment on 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 ([34]).

([32]) 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).

([33]) 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.

([34]) See EDPS Opinion of 10 April 2007 on the financing of the common agricultural policy (OJ C 134, 16.6.2007, p. 1).

53. Thirdly, while the CRA Regulation does not specify the medium on which the information should be published, in practice, it is imaginable that the publication will take place on 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 ([35]).

54. In view of the above, it is necessary to oblige ESMA 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 ([36]). 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 ([37]).

2.4.5. *Conclusion regarding disclosure of information regarding periodic penalty payments*

55. The EDPS is of the view that the provision on the mandatory publication of periodic penalty payments — as it is currently drafted — 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.

3. **CONCLUSIONS**

56. The EDPS makes the following recommendations:

— inserting a substantial provision in the CRA Regulation with the following wording: 'With regard to the processing of personal data carried out by Member States within the framework of this Regulation, competent authorities and sectoral competences authorities shall apply the provisions of national rules implementing 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',

— adding specific safeguards to Article 34 of the CRA Regulation, 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, the assurance of 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,

— clearly specify the categories of telephone and data traffic records which CRAs are required to retain and/or to provide to ESMA. Such data must be adequate relevant and not excessive in relation to the purpose for which they are processed,

— make explicit that access to telephone and data traffic directly from telecom providers is excluded,

([35]) 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

([36]) 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.

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

— limit access to records of telephone and data traffic to 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,

— assess the necessity of the proposed system for the mandatory publication of periodic penalty payments and verify whether the publication obligation does not go 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.

Done at Brussels, 10 February 2012.

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor