

# Official Journal of the European Union

C 279



English edition

## Information and Notices

Volume 54

23 September 2011

| Notice No     | Contents                                                                                                                                                                                                                                                                                             | Page |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| I             | <i>Resolutions, recommendations and opinions</i>                                                                                                                                                                                                                                                     |      |
|               | OPINIONS                                                                                                                                                                                                                                                                                             |      |
|               | <b>European Data Protection Supervisor</b>                                                                                                                                                                                                                                                           |      |
| 2011/C 279/01 | Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)                                                                                                    | 1    |
| 2011/C 279/02 | Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (Euratom) No 1074/1999 | 11   |
| 2011/C 279/03 | Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council on energy market integrity and transparency                                                                                                                        | 20   |
| II            | <i>Information</i>                                                                                                                                                                                                                                                                                   |      |
|               | INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES                                                                                                                                                                                                                           |      |
|               | <b>European Commission</b>                                                                                                                                                                                                                                                                           |      |
| 2011/C 279/04 | Non-opposition to a notified concentration (Case COMP/M.6349 — Motherson/Cross Industries/Peguform/Wethje) <sup>(1)</sup>                                                                                                                                                                            | 28   |

EN

Price:  
EUR 3<sup>(1)</sup> Text with EEA relevance

(Continued overleaf)

| <u>Notice No</u> | Contents (continued)                                                                                                      | Page |
|------------------|---------------------------------------------------------------------------------------------------------------------------|------|
| 2011/C 279/05    | Non-opposition to a notified concentration (Case COMP/M.6218 — Ineos/Tessenderlo Group S-PVC Assets) <sup>(1)</sup> ..... | 28   |

---

#### IV *Notices*

##### NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

##### **European Commission**

|               |                           |    |
|---------------|---------------------------|----|
| 2011/C 279/06 | Euro exchange rates ..... | 29 |
|---------------|---------------------------|----|

---

#### V *Announcements*

##### ADMINISTRATIVE PROCEDURES

##### **European Commission**

|               |                                                                                                                                                                                                                                                                            |    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 2011/C 279/07 | MEDIA 2007 — Development, distribution, promotion and training — Call for proposals — EACEA/21/11 — Support for the development of production projects — Animation, creative documentaries and drama — Single Projects, Slate Funding and Slate Funding second stage ..... | 30 |
| 2011/C 279/08 | MEDIA 2007 — Development, distribution, promotion and training — Call for proposals — EACEA/22/11 — Support for the development of on- and off-line interactive works .....                                                                                                | 33 |

##### PROCEDURES RELATING TO THE IMPLEMENTATION OF COMPETITION POLICY

##### **European Commission**

|               |                                                                                                                                      |    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------|----|
| 2011/C 279/09 | Prior notification of a concentration (Case COMP/M.6348 — Arla Foods/Allgäuland) <sup>(1)</sup> .....                                | 36 |
| 2011/C 279/10 | Prior notification of a concentration (Case COMP/M.6392 — Gores/Mexx) — Candidate case for simplified procedure <sup>(1)</sup> ..... | 37 |




---

<sup>(1)</sup> Text with EEA relevance

## I

*(Resolutions, recommendations and opinions)*

## OPINIONS

## EUROPEAN DATA PROTECTION SUPERVISOR

**Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)**

(2011/C 279/01)

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 Article 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 <sup>(1)</sup>,

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector <sup>(2)</sup>,

Having regard to Regulation (EC) No 45/2001 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 <sup>(3)</sup>, and in particular Article 41 thereof,

HAS ADOPTED THE FOLLOWING OPINION

**I. INTRODUCTION****I.1. Publication of the report**

1. On 18 April 2011, the Commission presented its evaluation report on the Data Retention Directive (hereafter: 'the Evaluation report') <sup>(4)</sup>. The Evaluation report was sent for information to the EDPS on the same day. For the reasons set out in part I.2 below, the EDPS

issues the present Opinion on his own initiative, in accordance with Article 41 of Regulation (EC) No 45/2001.

2. Before the adoption of the Communication the EDPS was given the possibility to provide informal comments. The EDPS is pleased to see that several of these comments have been taken into account by the Commission when drafting the final version of the document.
3. The Commission has prepared the Evaluation report to meet its obligation in Article 14 of the Data Retention Directive to evaluate the application of the Directive and its impact on economic operators and consumers, with a view to determining whether it is necessary to amend the provisions of the Directive <sup>(5)</sup>. The EDPS is pleased to see that, although not strictly required by Article 14, the Commission also took into account in the report 'the implications of the Directive for fundamental rights, in view of the criticisms which have been levelled in general at data retention' <sup>(6)</sup>.

**I.2. Reasons for and aim of the current EDPS Opinion**

4. The Data Retention Directive constituted an EU response to urgent security challenges, following the major terrorist attacks in Madrid in 2004 and in London in 2005. Despite the legitimate purpose for setting up a data retention scheme, criticism was voiced in relation to the huge impact the measure had on the privacy of citizens.
5. The obligation to retain data in accordance with the Data Retention Directive allows competent national authorities to retrace telephone and Internet behaviour of all persons in the EU whenever they use telephone or Internet up to a period of two years.

<sup>(1)</sup> OJ L 281, 23.11.1995, p. 31.

<sup>(2)</sup> OJ L 201, 31.7.2002, p. 37 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337, 18.12.2009, p. 11.

<sup>(3)</sup> OJ L 8, 12.1.2001, p. 1.

<sup>(4)</sup> COM(2011) 225 final.

<sup>(5)</sup> The Data Retention Directive (Directive 2006/24/EC) was adopted on 15 March 2006 and published in OJ L 105, 13.4.2006, p. 54. The deadline for issuing the report was set at 15 September 2010, see Article 14(1) of the Data Retention Directive.

<sup>(6)</sup> See p. 1 of the Evaluation report.

6. The retention of telecommunications data clearly constitutes an interference with the right to privacy of the persons concerned as laid down by Article 8 of the European Convention of Human Rights (hereafter: 'ECHR') and Article 7 of the EU Charter of Fundamental Rights.
7. The European Court of Human Rights (hereafter: 'ECtHR') has repeatedly stated that the 'mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [ECHR]' (7). With regard to telephone data in particular, the ECtHR has stated that 'release of that information to the police without the consent of the subscriber also amounts [...] to an interference with a right guaranteed by Article 8 [ECHR]' (8).
8. It follows from Article 8(2) of the ECHR and Article 52(1) of the EU Charter of Fundamental Rights that an interference may be justified if it is provided for by law, serves a legitimate aim and is necessary in a democratic society for achieving that legitimate aim.
9. The EDPS has acknowledged that the availability of certain traffic and location data can be crucial for law enforcement agencies in the combat of terrorism and other serious crime. However, at the same time, the EDPS has repeatedly expressed doubts about the justification for retaining data on such a scale in light of the rights to privacy and data protection (9). These doubts have been shared by many civil society organisations (10).
10. The EDPS has been closely following the creation, implementation and evaluation of the Directive since 2005 in different ways. The EDPS issued a critical Opinion in 2005, after the Commission published its proposal for the Directive (11). After the adoption of the Directive, the EDPS became member of the Data Retention Expert Group, referred to in recital 14 of the Data Retention Directive (12). Furthermore, the EDPS participates in the work of the Article 29 Working Party, which published several documents on the matter, the most recent one from July 2010 being a report about how the Directive has been applied in practice (13). Finally, the EDPS acted as intervener in a case before the European Court of Justice in which the validity of the Directive was challenged (14).
11. The importance of the Evaluation report and the evaluation process cannot be overstated (15). The Data Retention Directive constitutes a prominent example of an EU measure aiming at ensuring availability of data generated and processed in the context of electronic communications for law enforcement activities. Now that the measure has been in place for several years, an evaluation of its practical application should actually demonstrate the necessity and proportionality of the measure in light of the rights to privacy and data protection. In this respect the EDPS has called the evaluation 'the moment of truth' for the Data Retention Directive (16).
12. The current evaluation process also has implications for other instruments regulating information management, including the processing of huge amounts of personal data, in the area of freedom, security and justice. In a Communication of 2010, the Commission concluded that the evaluation mechanisms of the various instruments show a wide variety (17). The EDPS believes that the current evaluation procedure should be used to set the standard for the evaluation of other EU instruments and ensure that only those measures stay in place that are truly justified.
13. Against this background, the EDPS wishes to share his reflections on the findings presented in the Evaluation report in a public Opinion. This is done at an early stage of the process in order to provide an effective and constructive contribution to the discussions to come, possibly in the context of a new legislative proposal as referred to by the Commission in the Evaluation report (18).

### 1.3. Structure of the Opinion

14. The present Opinion will analyse and discuss the content of the Evaluation report from a privacy and data protection point of view. The analysis will focus on whether the current Data Retention Directive meets the requirements set out by these two fundamental rights. This includes an analysis of whether the necessity of data retention as regulated in the Directive has sufficiently been demonstrated.

15. The present Opinion is organised as follows. Part II will present the main content of the Data Retention Directive

(7) See f.i. ECHR of 4 December 2008, *S. and Marper v. UK*, 30562/04 and 30566/04, paragraph 67.

(8) See ECHR of 2 August 1984, *Malone v. UK*, A-82, paragraph 84.

(9) See the EDPS Opinion of 26 September 2005, OJ C 298, 29.11.2005, p. 1. During a conference organised by the Commission in December 2010, the EDPS referred to the instrument as 'the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects', see speech of 3 December 2010, to be found on the EDPS website (<http://www.edps.europa.eu>) under 'Publications' >> 'Speeches & Articles' >> '2010'.

(10) See in that respect the letter of 22 June 2010 from a large group of civil society organisations to Commissioners Malmström, Reding and Kroes ([http://www.vorratsdatenspeicherung.de/images/DRletter\\_Malmstroem.pdf](http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf)).

(11) See the EDPS Opinion referred to in footnote 9.

(12) See furthermore Commission Decision of 25 March 2008, OJ L 111, 23.4.2008, p. 11.

(13) See WP 172 of 13 July 2010, Report 1/2010 on the second joint enforcement action.

(14) See ECJ of 10 February 2009, *Ireland v. Parliament and Council*, C-301/06. See on the case also point 29 below.

(15) In his Opinion of 2005, the EDPS already emphasised the importance of the obligation to evaluate the instrument (see footnote 9, points 72-73).

(16) See the speech of 3 December 2010 referred to in footnote 9.

(17) COM(2010) 385 of 20 July 2010, Overview of information management in the area of freedom, security and justice, p. 24. See on this Communication the EDPS Opinion of 30 September 2010, to be found on the EDPS website (<http://www.edps.europa.eu>) under 'Consultation' >> 'Opinions' >> '2010'.

(18) See p. 32 of the Evaluation report.

and its relationship with Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (hereafter: 'the ePrivacy Directive')<sup>(19)</sup>. Part III will briefly set out the changes brought about by the Lisbon Treaty, as these are particularly relevant for the current matter and have direct consequences for the way in which EU rules on data retention should be perceived, evaluated and possibly revised. The largest part of the Opinion, Part IV, contains the analysis on the validity of the Data Retention Directive in light of the rights to privacy and data protection and with a view to the findings presented in the Evaluation report. Part V will discuss the possible ways forward. The Opinion ends, in part VI, with a conclusion.

## II. THE EU RULES ON DATA RETENTION

16. In the context of the present Opinion, data retention refers to the obligation put on the providers of publicly available electronic communications services or of public communications networks to retain traffic and location data, as well as related data necessary to identify the subscriber or user for a certain period. This obligation is laid down in the Data Retention Directive, which further specifies in Article 5(1) the categories of data to be retained. According to Article 6 of the Directive, Member States ensure that these data are retained for a period of not less than six months and not more than two years from the date of the communication.
17. The data are to be retained to the extent that those data are generated or processed by the providers in the process of supplying the communication services concerned (Article 3). It also includes data related to unsuccessful call attempts. No data revealing the content of communications may be retained pursuant to the Directive (Article 5(1)).
18. The data are retained in order to ensure that the data are available for the purpose of 'the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law' (Article 1(1)).
19. The Data Retention Directive contains no further rules on the conditions under which competent national authorities can access the retained data. This is left to the discretion of the Member States and falls outside the scope of the Directive. Article 4 of the Directive underlines that these national rules should be in accordance with necessity and proportionality requirements as provided by, in particular, the ECHR.

20. The Data Retention Directive relates closely to the ePrivacy Directive. This Directive, which particularises and

complements the general Data Protection Directive 95/46/EC, determines that Member States should ensure the confidentiality of communications and related traffic data<sup>(20)</sup>. The ePrivacy Directive requires that traffic and location data generated by using electronic communications services must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except where and only for so long as, they are needed for billing purposes<sup>(21)</sup>. Subject to consent, certain data may be processed for the duration necessary for the provision of a value-added service.

21. On the basis of Article 15(1) of the ePrivacy Directive, it is possible for Member States to adopt legislative measures to restrict the scope of the obligations mentioned above if it 'constitutes 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 [...]'. The issue of data retention is explicitly referred to in Article 15(1) of the ePrivacy Directive. Member States may 'adopt legislative measures providing for the retention of data for a limited period' justified on the grounds mentioned.
22. The Data Retention Directive was intended to align Member States' initiatives under Article 15(1), as far as it concerns retention of data for the investigation, detection and prosecution of serious crime. It should be emphasised that the Data Retention Directive constitutes an exception to the general obligation enshrined in the ePrivacy Directive to erase the data when they are no longer needed<sup>(22)</sup>.
23. With the adoption of the Data Retention Directive an extra paragraph 1(a) was inserted in Article 15 of the ePrivacy Directive, in which it is stated that paragraph 15(1) shall not apply to data specifically required by the Data Retention Directive to be retained for the purposes referred to in Article 1(1) of that Directive.
24. It is noted in the Evaluation report, as will be further discussed in Part IV.3 below, that Articles 15(1) and 15(1)(b) have been used by several Member States to use data retained under the Data Retention Directive also for other purposes<sup>(23)</sup>. The EDPS has referred to this as a 'legal loophole' in the legal framework, which hampers the purpose of the Data Retention Directive, namely to create a level-playing field for industry<sup>(24)</sup>.

<sup>(20)</sup> See Article 5 of the ePrivacy Directive.

<sup>(21)</sup> See Articles 6 and 9 of the ePrivacy Directive.

<sup>(22)</sup> See also the WP 29 in the Report of 13 July 2010, referred to in footnote 13, p. 1.

<sup>(23)</sup> See p. 4 of the Evaluation report. See in this respect also recital 12 of the Data Retention Directive.

<sup>(24)</sup> See the speech of 3 December 2010 referred to in footnote 9, p. 4.

<sup>(19)</sup> See footnote 2.



### III. GENERAL EU LEGAL CONTEXT HAS CHANGED AFTER LISBON

25. The general EU legal context relevant for the Data Retention Directive has changed considerably with the entry into force of the Lisbon Treaty. A major change was the abolition of the pillar structure, which had established different legislative procedures and review mechanisms for the different areas of EU competence.
26. The previous pillar structure regularly raised discussions about the correct legal basis of an EU instrument in case a subject matter triggered EU competence in the different pillars. The choice of a legal basis was not without importance as it led to different legislative procedures with regard to, for instance, the voting requirements in Council (qualified majority or unanimity) or the involvement of the European Parliament.
27. These discussions were highly relevant for data retention. Since the Data Retention Directive aimed at harmonising the obligation for operators, and thereby at eliminating obstacles to the internal market, the legal basis could be found in Article 95 of the former EC Treaty (the former first pillar). However, the issue could have been approached from the law enforcement side, arguing that the purpose for storing the data was combating serious crimes, within the framework of police and judicial cooperation in criminal matters in the former EU Treaty (the former third pillar) <sup>(25)</sup>.
28. In the event, the Data Retention Directive was adopted on the basis of Article 95 of the former EC Treaty, regulating only the obligations for operators. The Directive did not include rules on the access and use of the retained data by law enforcement authorities.
29. After its adoption, the validity of the Directive was challenged before the Court of Justice. It was argued that the Directive should have been based on the third pillar instead of the first pillar, since the purpose for which the data were to be retained (the investigation, detection and prosecution of serious crime) fell under the EU competence in the third pillar <sup>(26)</sup>. However, since the conduct of the competent authorities was explicitly left outside the scope of the Directive, the Court of Justice concluded that the Directive was rightly based on the EC Treaty <sup>(27)</sup>.
30. From the start, the EDPS has argued that if the EU would adopt an instrument on data retention, it should regulate the obligation for operators as well as the access and further use by law enforcement authorities. In his Opinion of 2005 on the Commission proposal, the EDPS underlined that the access and further use by competent national authorities constituted an essential and inseparable part of the subject matter <sup>(28)</sup>.
31. As will be further elaborated below, the negative effects of the EU regulating only half of the matter have been confirmed by the present Evaluation report. The Commission concludes that the differences in national law on the access and further use by the competent national authorities have led to 'considerable difficulties' for operators <sup>(29)</sup>.
32. With the abolition of the pillar structure after the entry into force of the Lisbon Treaty, the two relevant areas of EU competences were put together in the TFEU which allows the adoption of EU legislation subject to the same legislative procedure. This new context would allow the adoption of a new, single instrument on data retention regulating the obligations for the operators as well as the conditions for access and further use by law enforcement authorities. As will be explained in Part IV.3 below, the rights to privacy and data protection require that if a revised EU measure on data retention is considered, it should at least regulate the matter in its entirety.
33. The Lisbon Treaty not only abolished the pillar structure, it also granted the previously non-binding EU Charter of Fundamental Rights, which included the rights to privacy and data protection in Articles 7 and 8, the same legal value as the Treaties <sup>(30)</sup>. A subjective right to data protection was furthermore included in Article 16 of the TFEU, creating a separate legal basis for EU instruments on the protection of personal data.
34. The protection of fundamental rights has since long been a cornerstone of EU policy, and the Lisbon Treaty has led to an even stronger commitment to these rights in the EU context. The changes brought about by the Lisbon Treaty inspired the Commission in October 2010 to announce the promotion of a 'fundamental rights culture' at all stages of the legislative process and to state that the EU Charter of Fundamental Rights 'should serve as a compass for the Union's policy' <sup>(31)</sup>. The EDPS believes that the current evaluation process offers the Commission a good opportunity to give proof of this commitment.

<sup>(25)</sup> A first proposal for EU rules on data retention (a framework decision) was based on the former EU Treaty, tabled by Ireland, France, Sweden and the United Kingdom. See Council document 8958/04 of 28 April 2004. This proposal was followed by a Commission proposal based on the EC Treaty. See COM(2005) 438 of 21 September 2005.

<sup>(26)</sup> This argument was based on the judgment of the Court of Justice in the 'PNR-cases', see ECJ of 30 May 2006, *Parliament v. Council and Commission*, C-317/05 and C-318/04.

<sup>(27)</sup> See ECJ of 10 February 2009, *Ireland v. Parliament and Council*, C-301/06, paragraphs 82-83.

<sup>(28)</sup> See the Opinion of 2005, point 80. See on this also part IV.3 of the present Opinion.

<sup>(29)</sup> See p. 31 of the Evaluation report.

<sup>(30)</sup> See Article 6(1) of the TEU.

<sup>(31)</sup> COM(2010) 573 of 19 October 2010, Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, p. 4.

#### IV. DOES THE DATA RETENTION DIRECTIVE MEET PRIVACY AND DATA PROTECTION REQUIREMENTS?

35. The Evaluation report brings to light several weaknesses of the present Data Retention Directive. The information provided in the report shows that the Directive has failed to meet its main purpose, namely to harmonise national legislation concerning data retention. The Commission notes that there are 'considerable' differences between transposing legislation in the areas of purpose limitation, access to data, periods of retention, data protection and data security and statistics<sup>(32)</sup>. According to the Commission, the differences are partly due to the variation explicitly provided for by the Directive. The Commission states, however, that even beyond this, 'differences in national application of data retention have presented considerable difficulties for operators' and that there 'continues to be a lack of legal certainty for industry'<sup>(33)</sup>. It goes without saying that such a lack of harmonisation is detrimental to all parties involved: citizens, business operators, as well as law enforcement authorities.

36. From a privacy and data protection perspective, the Evaluation report also justifies the conclusion that the Data Retention Directive does not meet the requirements imposed by the rights to privacy and data protection. There are several deficiencies: the necessity of data retention as provided for in the Data Retention Directive has not been sufficiently demonstrated, data retention could, in any event, have been regulated in a less privacy-intrusive way, and the Data Retention Directive lacks 'foreseeability'. These three points will be further elaborated below.

##### IV.1. The necessity of data retention as provided for in the Data Retention Directive has not sufficiently been demonstrated

37. An interference with the rights to privacy and data protection is allowed only if the measure is necessary for achieving the legitimate aim. The necessity of data retention as a law enforcement measure has constantly been a major point of discussion<sup>(34)</sup>. In the proposal for the Directive it was stated that the limitations on the rights to privacy and data protection were 'necessary to meet the generally recognised objectives of preventing and combating crime and terrorism'<sup>(35)</sup>. However, in the Opinion of 2005, the EDPS indicated not to be convinced by this statement, since it required further evidence<sup>(36)</sup>. Still, without the provision of any additional evidence it was stated in recital 9 of the Data Retention Directive that 'retention of data has proved to be [...] a necessary and effective investigative tool for law enforcement in several Member States'.

38. Due to the lack of sufficient evidence the EDPS argued that the Data Retention Directive was only based on the assumption that data retention as developed in the Data Retention Directive constituted a necessary measure<sup>(37)</sup>. The EDPS therefore called upon the Commission and the Member States to use the occasion of the Evaluation report to provide further evidence which confirmed that the assumption on the necessity of the measure of data retention and the way it is regulated in the Data Retention Directive was indeed correct.

39. On this point, the Commission states in the Evaluation report that '[m]ost Member States take the view that EU rules on data retention remain necessary as a tool for law enforcement, the protection of victims and the criminal justice systems'. Data retention is furthermore referred to as playing a 'very important role' in criminal investigation, as being 'at least valuable and in some cases indispensable' and it is stated that without data retention certain criminal offences 'might never have been solved'<sup>(38)</sup>. The Commission concludes that the EU should therefore 'support and regulate data retention as a security measure'<sup>(39)</sup>.

40. It is, however, doubtful whether the Commission can indeed conclude that most Member States consider data retention a necessary tool. It is not indicated which Member States constitute the majority, which in an EU of 27 Member States should be at least 14 in order to be able to speak about most Member States. The number of Member States concretely referred to in Chapter 5, on which the conclusions are based, is at most nine<sup>(40)</sup>.

41. Furthermore, it seems that the Commission bases itself mainly on statements of Member States on whether they consider data retention a necessary tool for law enforcement purposes. These statements, however, rather indicate that the Member States concerned like to have EU rules on data retention, but cannot as such establish the need for data retention as a law enforcement measure, supported and regulated by the EU. The statements on the necessity should be supported by sufficient evidence.

42. Admittedly, demonstrating the necessity of a privacy intrusive measure is not an easy task. Especially not for the Commission, that largely depends on information provided by the Member States.

43. However, if a measure is already in place, such as the Data Retention Directive, and practical experience has been gained, there should be sufficient qualitative and

<sup>(32)</sup> See p. 31 of the Evaluation report.

<sup>(33)</sup> See p. 31 of the Evaluation report.

<sup>(34)</sup> See the EDPS Opinion of 2005. See also the letter of 22 June 2010 from a large group of civil society organisations, referred to in footnote 10.

<sup>(35)</sup> COM(2005) 438 of 21 September 2005, p. 3.

<sup>(36)</sup> See the Opinion of 2005, points 17-22.

<sup>(37)</sup> See the speech of 3 December 2010 referred to in footnote 9.

<sup>(38)</sup> All quotes are from p. 23 or 31 of the Evaluation report.

<sup>(39)</sup> See p. 31 of the Evaluation report.

<sup>(40)</sup> Czech Republic, Germany, Ireland, Hungary, Netherlands, Poland, Slovenia, Finland and United Kingdom.

quantitative information available which allows an assessment of whether the measure is actually working and whether comparable results could have been achieved without the instrument or with alternative, less privacy-intrusive means. Such information should constitute genuine proof and show the relationship between use and result<sup>(41)</sup>. As it concerns an EU Directive, the information should furthermore represent the practice of at least a majority of EU Member States.

44. After careful analysis, the EDPS takes the view that, although the Commission has clearly put much effort into collecting information from the Member States' governments, the quantitative and qualitative information provided by the Member States is not sufficient to confirm the necessity of data retention as it is developed in the Data Retention Directive. Interesting examples of its use have been provided; however, there are simply too many shortcomings in the information presented in the report to allow general conclusions on the necessity of the instrument. Moreover, further investigation into alternative means should still be done. These two points will now be further elaborated.

*The quantitative and qualitative information provided in the Evaluation report*

45. As regards the quantitative, statistical information presented mainly in Chapter 5 and the Annex to the Evaluation report, crucial information is missing. For instance, the statistics do not indicate the purposes for which the data were sought. Furthermore, the numbers do not reveal whether all data to which access has been requested were data which were stored as a consequence of the legal obligation to retain data or for business purposes. Also, no information is provided on the results of the use of data. For drawing conclusions, it is furthermore problematic that the information from the different Member States is not always fully comparable and that in many cases the charts represent only nine Member States.
46. The qualitative examples provided in the report serve as a better illustration of the important role retained data has played in certain specific situations and for the potential benefits of a system of data retention. However, it is not in all cases clear whether use of the retained data was the only means to solve the crime involved.
47. Some examples illustrate the indispensability of the measure of data retention for combating cybercrime. In this respect it is worth noting that the main international instrument in this field, the Council of Europe Cybercrime Convention, does not foresee data retention as a measure to combat cybercrime, but refers only to data preservation as an investigative tool<sup>(42)</sup>.
48. The Commission seems to attach considerable weight to examples provided by the Member States in which

retained data was used to exclude suspects from crime scenes and to verify alibis<sup>(43)</sup>. Although these are interesting examples of how the data is used by law enforcement authorities, they cannot be put forward as demonstrating the need for data retention. This argument should be used with caution as it might be misunderstood, implying that retention of data is necessary for proving the innocence of citizens, which would be difficult to reconcile with the presumption of innocence.

49. The Evaluation report only briefly discusses the value of data retention in relation to technological developments, and more specifically the use of prepaid SIM cards<sup>(44)</sup>. The EDPS underlines that more quantitative and qualitative information on the use of new technologies not covered by the Directive (this may be the case for VoIP and social networks) would have been instructive for assessing the effectiveness of the Directive.
50. The Evaluation report is limited because it mostly focuses on quantitative and qualitative information provided by the Member States that have implemented the Data Retention Directive. It would however have been interesting to see whether any considerable differences occurred between those Member States and Member States that have not implemented the Directive. Especially for those Member States in which implementing legislation has been annulled (Czech Republic, Germany and Romania) it would have been interesting to see whether there is any evidence of the rise or fall of successful criminal investigations, either before or after these annulments.
51. The Commission acknowledges that the statistics and examples provided in the Evaluation report are 'limited in some respects', but nevertheless concludes that the evidence attests to 'the very important role of retained data for criminal investigations'<sup>(45)</sup>.
52. The EDPS feels that the Commission should have been more critical towards the Member States. As explained, political statements by some Member States on the need for such a measure cannot alone justify EU action. The Commission should have insisted that Member States provide sufficient evidence that demonstrates the necessity of the measure. According to the EDPS, the Commission should have at least made its support for data retention as a security measure (see p. 31 of the Evaluation report) subject to the condition that Member States provide further evidence during the impact assessment.

*Alternative means*

53. The necessity for data retention as set forth in the Data Retention Directive also depends on whether less privacy-intrusive alternative means exist which might have led to comparable results. This has been confirmed by the Court of Justice in its *Schecke* ruling in November 2010, in which EU legislation on the publication of names of beneficiaries

<sup>(41)</sup> See on the principle of necessity and proportionality also the EDPS Opinion of 25 March 2011 on the EU PNR proposal, to be found on the EDPS website (<http://www.edps.europa.eu>) under 'Consultation' >> 'Opinions' >> '2011'.

<sup>(42)</sup> See also p. 5 of the Evaluation report.

<sup>(43)</sup> See p. 24 of the Evaluation report.

<sup>(44)</sup> See p. 25 of the Evaluation report.

<sup>(45)</sup> See p. 31 of the Evaluation report.



of agricultural funds was annulled<sup>(46)</sup>. One of the reasons for annulment was that the Council and the Commission had not considered alternative measures which would be consistent with the objective of the publication while at the same time causing less interference with the right to privacy and data protection of the persons concerned<sup>(47)</sup>.

54. The main alternative put forward in the discussions surrounding the Data Retention Directive is the method of data preservation ('quick freeze' and 'quick freeze plus')<sup>(48)</sup>. It consists of temporarily securing or 'freezing' of certain telecommunications traffic and location data relating only to specific suspects of criminal activity, which may subsequently be made available to law enforcement authorities with a judicial authorisation.
55. Data preservation is mentioned in the Evaluation report in the context of the aforementioned Cybercrime Convention, but it is considered as inappropriate because it 'does not guarantee the ability to establish evidence trails prior to the preservation order, and does not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime'<sup>(49)</sup>.
56. The EDPS acknowledges that less information is available when a system of data preservation is used instead of a broad system of data retention. However, it is precisely because of its more targeted nature that data preservation constitutes a less privacy-intrusive instrument in terms of scale and number of people it affects. The assessment should not only focus on the available data, but also on the different results achieved with both systems. The EDPS considers a more in-depth investigation into this measure justified and indispensable. This could be done during the impact assessment in the months to come.
57. In that respect, it is unfortunate that in the conclusions of the report the Commission commits itself to examining whether — and if so how — an EU approach on data preservation might complement (i.e. not replace) data retention<sup>(50)</sup>. The possibility of combining any kind of retention scheme with the procedural safeguards surrounding various ways of data preservation indeed deserves further investigation. However, the EDPS recommends the Commission during the impact assessment also to consider whether a system of data preservation, or other alternative means, could fully or partly substitute the current data retention scheme.

<sup>(46)</sup> ECJ of 9 November 2010, *Volker und Markus Schecke*, C-92/09 and C-93/09.

<sup>(47)</sup> ECJ, *Schecke*, paragraph 81.

<sup>(48)</sup> 'Quick freeze' concerns the 'freezing' of traffic and location data relating to a specific suspect as from the date of the judicial authorisation. 'Quick freeze plus' also includes the 'freezing' of data already held by operators for billing and transmission purposes.

<sup>(49)</sup> See p. 5 of the Evaluation report.

<sup>(50)</sup> See p. 32 of the Evaluation report.

#### IV.2. Data retention as regulated in the Data Retention Directive, in any event, goes beyond what is necessary

58. According to the EDPS, the information in the Evaluation report does not contain sufficient evidence to demonstrate the necessity of the data retention measure as laid down in the Data Retention Directive. However, the Evaluation report does permit the conclusion that the Data Retention Directive has regulated data retention in a way which goes beyond what is necessary, or, at least, has not ensured that data retention has not been applied in such a way. In that respect, four elements can be highlighted.
59. In the first place, the unclear purpose of the measure and the wide notion of 'competent national authorities' has led to the use of retained data for far too wide a range of purposes and by far too many authorities. Furthermore, there is no consistency in the safeguards and conditions for access to the data. For instance, access is not made subject to prior approval by a judicial or other independent authority in all Member States.
60. In the second place, the maximum retention period of two years appears to go beyond what is necessary. Statistical information from a number of Member States in the Evaluation report shows that the large majority of access requests relate to data up to six months, namely 86 %<sup>(51)</sup>. Furthermore, 16 Member States have chosen a retention period of 1 year or less in their legislation<sup>(52)</sup>. This strongly suggests that a maximum period of two years goes far beyond what is considered necessary by the majority of Member States.
61. Furthermore, the lack of a fixed single retention period for all Member States has created a variety of diverging national laws which may trigger complications, because it is not always evident what national law — on data retention as well as on data protection — is applicable when operators store data in a Member State other than the one in which the data are collected.
62. In the third place, the level of security is not sufficiently harmonised. One of the main conclusions of the Article 29 Working Party in its report of July 2010 was that there is a patchwork of security measures in place in the different Member States. The Commission seems to consider the security measures in the current Directive as sufficient, as 'there are no concrete examples of serious breaches of privacy'<sup>(53)</sup>. It appears however that the Commission has only asked Member States' governments to report on this. In order to evaluate the suitability of present security rules and measures, a broader consultation and more concrete investigation into instances of abuse is needed. Even if no

<sup>(51)</sup> See p. 22 of the Evaluation report. 12 % concerns data between six and twelve months old and 2 % relates to data older than one year.

<sup>(52)</sup> See p. 14 of the Evaluation report.

<sup>(53)</sup> See p. 30 of the Evaluation report.

specific instances of security breaches are mentioned in the context of the report, data security breaches and scandals in the area of traffic data and electronic communications in some Member States also serve as illustrative warnings. This issue cannot be taken lightly, as the security of the retained data is of crucial importance to a system of data retention as such, as it ensures respect for all other safeguards<sup>(54)</sup>.

63. In the fourth place, it is not clear from the report whether all categories of retained data have proven to be necessary. Only some general distinctions are made between telephone and Internet data. Some Member States have chosen to impose a shorter period of retention for Internet data<sup>(55)</sup>. However, no general conclusions can be drawn from that.

#### IV.3. The Data Retention Directive lacks foreseeability

64. Another shortcoming of the Data Retention Directive concerns its lack of foreseeability. The requirement of foreseeability stems from the general requirement in Article 8(2) of the ECHR and Article 52(1) of the EU Charter of Fundamental Rights that an interference should be provided for by law. According to the ECtHR, it means that the measure should have a legal basis in law and should be compatible with the rule of law. This implies that the law is adequately accessible and foreseeable<sup>(56)</sup>. It has also been underlined by the Court of Justice in its *Österreichischer Rundfunk* ruling that the law should be formulated with sufficient precision to enable the citizens to adjust their conduct accordingly<sup>(57)</sup>. The law must indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise<sup>(58)</sup>.

65. Also in the checklist set out in the Commission Communication on the EU Charter of Fundamental Rights, one of the questions to be answered is whether any limitation of fundamental rights is formulated in 'a clear and predictable manner'<sup>(59)</sup>. In its Communication on the overview of information management in the area of freedom, security and justice, the Commission has also stated that citizens 'have right to know what personal data are processed and exchanged about them by whom and for what purpose'<sup>(60)</sup>.

66. In the case of an EU Directive, the responsibility for compliance with fundamental rights, including the requirement of foreseeability, lies primarily with the Member States which implement the Directive in their

national legislation. It is a well-known requirement that such implementation should respect for fundamental rights<sup>(61)</sup>.

67. Also in the Evaluation report the Commission underlines that the Directive 'does not in itself guarantee that retained data are being stored, retrieved and used in full compliance with the right to privacy and protection of personal data'. It recalls that the 'responsibility for ensuring these rights are upheld lies with Member States'<sup>(62)</sup>.
68. However, the EDPS believes that an EU Directive itself should to a certain extent also fulfil the requirement of foreseeability. Or, to rephrase the Court of Justice in *Lindqvist*, the regime a Directive provides should not 'lack predictability'<sup>(63)</sup>. Such is especially the case with an EU measure which requires Member States to organise a large-scale interference with the rights to privacy and data protection of citizens. The EDPS takes the view that the EU has a responsibility to ensure at least a clearly defined purpose and a clear indication of who can get access to the data and under which conditions.
69. This position is endorsed by the new legal context created by the Lisbon Treaty, which, as explained, enhanced EU competence in the field of police and judicial cooperation in criminal matters and established a stronger commitment of the EU to uphold fundamental rights.
70. The EDPS wishes to recall that the requirement of a specified purpose and the subsequent prohibition to process data in a way incompatible with that purpose ('purpose limitation principle') are of fundamental importance to the protection of personal data, as is confirmed by Article 8 of the EU Charter of Fundamental Rights<sup>(64)</sup>.
71. The Evaluation report shows that the choice of leaving the precise definition of what constitutes a 'serious crime' and subsequently of what should be considered as 'competent authorities' to the discretion of the Member States, has led to a wide variety of purposes for which the data have been used<sup>(65)</sup>.

72. The Commission states that '[m]ost transposing Member States, in accordance with their legislation, allow the access and use of retained data for purposes going beyond those covered by the Directive, including preventing and combating crime generally and the risk of life and limb'<sup>(66)</sup>. Member States make use of the 'legal loophole' provided for in Article 15(1) of the ePrivacy Directive<sup>(67)</sup>. The Commission considers that this

<sup>(54)</sup> See on this also the EDPS Opinion of 2005, point 29-37. See also the speech of the Assistant Supervisor of 4 May 2011 to be found on the EDPS website (<http://www.edps.europa.eu>) under 'Publications' >> 'Speeches & Articles' >> '2011'.

<sup>(55)</sup> See p. 14 of the Evaluation report.

<sup>(56)</sup> See ECtHR, *S. and Marper*, referred to in footnote 7, paragraph 151.

<sup>(57)</sup> ECJ of 20 May 2003, *Österreichischer Rundfunk*, C-465/00, paragraph 77, and ECtHR, *S. and Marper*, referred to in footnote 7, paragraph 95.

<sup>(58)</sup> See ECtHR, *Malone*, referred to in footnote 8, paragraphs 66-68.

<sup>(59)</sup> COM(2010) 573, referred to in footnote 31, p. 5.

<sup>(60)</sup> COM(2010) 385, referred to in footnote 17, p. 3.

<sup>(61)</sup> See, for example, ECJ of 6 November 2003, *Lindqvist*, paragraph 87.

<sup>(62)</sup> See p. 31 of the Evaluation report.

<sup>(63)</sup> ECJ, *Lindqvist*, paragraph 84.

<sup>(64)</sup> See also Article 6 of Directive 95/46/EC.

<sup>(65)</sup> See p. 8 of the Evaluation report.

<sup>(66)</sup> See p. 8 of the Evaluation report.

<sup>(67)</sup> As discussed in point 24 above.

situation may not provide sufficiently for the 'foreseeability which is a requirement in any legislative measure which restricts the right to privacy' <sup>(68)</sup>.

73. In these circumstances it cannot be said that the Data Retention Directive itself, read in particular in conjunction with the ePrivacy Directive, provides the clarity needed to fulfil the principle of foreseeability at EU level.

#### V. THE WAY FORWARD: ALL OPTIONS SHOULD BE CONSIDERED

74. The analysis in the previous part justifies the conclusion that the Data Retention Directive does not meet the requirements set out by the rights to privacy and data protection. It is therefore clear that the Data Retention Directive cannot continue to exist in its present form. In that respect, the Commission rightly proposes a revision of the current data retention framework <sup>(69)</sup>.

75. However, before proposing a revised version of the Directive:

- (a) the Commission should, during the impact assessment, invest in collecting further practical evidence from the Member States in order to demonstrate the necessity of data retention as a measure under EU law;
- (b) if a majority of Member States considers data retention to be necessary, these Member States should all provide the Commission with quantitative and qualitative evidence demonstrating it;
- (c) Member States that oppose such a measure of data retention should provide the Commission with information to enable a broader assessment of the matter.

76. In the impact assessment it should furthermore be examined whether alternative, less privacy-intrusive means could have led or could still lead to comparable results. The Commission should take the initiative on this, supported, if needed, by external expertise.

77. The EDPS is pleased to see that the Commission has announced the consultation of all stakeholders concerned during the impact assessment <sup>(70)</sup>. In this respect, the EDPS encourages the Commission to find ways to directly involve citizens in this exercise.

78. It should be underlined that an assessment of the necessity and the examination of alternative, less privacy-intrusive means can only be conducted in a fair way if all options for the future of the Directive are left open. In that respect, the Commission seems to exclude the possibility of repealing the Directive, either per se or combined with a proposal for an alternative, more targeted EU measure. The EDPS therefore calls upon the Commission to seriously consider these options in the impact assessment as well.

79. Only if there is agreement on the need for EU rules from the perspective of the internal market and police and judicial cooperation in criminal matters and if, during the impact assessment, the necessity of data retention, supported and regulated by the EU, can be sufficiently demonstrated, which includes a careful consideration of alternative measures, a future Data Retention Directive can be considered.

80. The EDPS does not deny the important value of retained data for law enforcement purposes and the crucial role it can play in specific cases. Like the German Bundesverfassungsgericht, the EDPS does not exclude that a well-defined obligation to retain telecommunications data may be justified under certain very strict conditions <sup>(71)</sup>.

81. Any future EU instrument on data retention should therefore meet the following basic requirements:

- it should be comprehensive and genuinely harmonise rules on the obligation to retain data, as well as on the access and further use of the data by competent authorities,
- it should be exhaustive, which means that it has a clear and precise purpose and that the legal loophole which exists with Article 15(1) of the ePrivacy Directive is closed,
- it should be proportionate and not go beyond what is necessary (see in that respect the comments made in Part IV.2 above).

82. Obviously, the EDPS will carefully scrutinise any future proposal on data retention in light of these basic conditions.

#### VI. CONCLUSION

83. The EDPS is pleased that, although not strictly required by Article 14 of the Data Retention Directive, the Commission also took into account in the Evaluation report the implications of the Directive for fundamental rights.

84. The Evaluation report shows that the Directive has failed to meet its main purpose, namely to harmonise national legislation concerning data retention. Such a lack of harmonisation is detrimental to all parties involved: citizens, business operators, as well as law enforcement authorities.

85. On the basis of the Evaluation report it may be concluded that the Data Retention Directive does not meet the requirements set out by the rights to privacy and data protection, for the following reasons:

- the necessity of data retention as provided for in the Data Retention Directive has not been sufficiently demonstrated,
- data retention could have been regulated in a less privacy-intrusive way,

<sup>(68)</sup> See p. 9 and 15 of the Evaluation report.

<sup>(69)</sup> See p. 32-33 of the Evaluation report.

<sup>(70)</sup> See p. 32-33 of the Evaluation report.

<sup>(71)</sup> See Bundesverfassungsgericht, 1 BvR 256/08.

- the Data Retention Directive lacks foreseeability.
86. The EDPS calls upon the Commission to consider seriously all options in the impact assessment including the possibility of repealing the Directive, either per se or combined with a proposal for an alternative, more targeted EU measure.
87. A future Data Retention Directive could be considered only if there were agreement on the need for EU rules from the perspective of the internal market and police and judicial cooperation in criminal matters and if, during the impact assessment, the necessity of data retention, supported and regulated by the EU, could be sufficiently demonstrated, which includes a careful consideration of alternative measures. Such an instrument should fulfil the following basic requirements:
- it should be comprehensive and genuinely harmonise rules on the obligation to retain data, as well as on the access and further use of the data by competent authorities,
  - it should be exhaustive, which means that it has a clear and precise purpose and the legal loophole which exists with Article 15(1) of the ePrivacy Directive is closed,
  - it should be proportionate and not go beyond what is necessary.
- Done at Brussels, 31 May 2011.
- Peter HUSTINX  
*European Data Protection Supervisor*
-

**Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (Euratom) No 1074/1999**

(2011/C 279/02)

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 <sup>(1)</sup>,

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 <sup>(2)</sup>, and in particular Article 28(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

## 1. INTRODUCTION

- On 17 March 2011, the Commission adopted a proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-fraud Office (OLAF) and repealing Regulation (Euratom) No 1074/1999 (hereinafter 'the Proposal').

### 1.1. Consultation with the EDPS

- The Proposal was sent by the Council to the EDPS on 8 April 2011. The EDPS understands this communication as a request to advise Community institutions and bodies, as foreseen in Article 28(2) of Regulation (EC) No 45/2001 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 (hereinafter 'Regulation (EC) No 45/2001'). The EDPS welcomes the explicit reference to this consultation in the preamble of the Proposal.

- The Proposal is aimed at amending Articles 1-14 and at deleting Article 15 of Regulation (EC) No 1073/1999. Council Regulation (Euratom) No 1074/1999 of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF) is expected to be repealed.
- Previously <sup>(3)</sup>, before the adoption of the Proposal, the EDPS was given the possibility by the Commission to provide informal comments. The EDPS welcomes the openness of the process, which has helped to improve the text from a data protection point of view at an early stage. Indeed, some of those comments have been taken into account in the Proposal.
- This new text is the result of a long review process. In 2006, the Commission put forward a proposal to amend Regulation (EC) No 1073/1999. The legislative proposal focused on 'achieving better operational efficiency and improved governance for the Office'.
- This previous proposal was discussed both in the Council and the European Parliament under the co-decision procedure. The EDPS issued his Opinion in April 2007, including many observations aimed at rendering the text of the proposal more coherent with the data protection rules enshrined in Regulation (EC) No 45/2001 <sup>(4)</sup>. The Parliament adopted a resolution on 20 November 2008 <sup>(5)</sup> in first reading including approximately one hundred amendments to the proposal.
- At the request of the Czech Presidency of the Council (January-June 2009), in July 2010 the Commission presented an updated Reflection paper on the reform of the Office to the European Parliament and the Council. In October 2010, the European Parliament welcomed the Reflection paper and asked the Commission to take up the legislative procedure again. On 6 December 2010, the

<sup>(1)</sup> OJ L 281, 23.11.1995, p. 31.

<sup>(2)</sup> OJ L 8, 12.1.2001 p. 1.

<sup>(3)</sup> In January 2011.

<sup>(4)</sup> Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ C 91, 26.4.2007, p. 1.

<sup>(5)</sup> European Parliament legislative resolution of 20 November 2008 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), P6\_TA-PROV(2008) 553.



Council adopted its Conclusions on the Reflection paper put forward by the Commission. The Supervisory Committee of OLAF contributed to the discussion with its opinions on the Reflection paper and on the respect for fundamental rights and procedural guarantees in investigations by OLAF. The Commission has thereafter presented the new Proposal.

### 1.2. The importance of the Proposal and the EDPS advice

8. The Proposal includes provisions which have a strong impact on individuals' rights. OLAF will continue to collect and further process sensitive data relating to suspected offences, offences, criminal convictions as well as information that would serve to exclude individuals from a right, benefit or contract insofar as such information represents a particular risk to the rights and freedoms of the data subjects. The fundamental right to the protection of personal data is relevant not only for its own sake, but also has strong connections with other fundamental rights, such as non-discrimination and due process of law, including the right of defence in OLAF investigations. The respect of due process has an impact on the validity of evidence and should be considered a priority by OLAF to reinforce its accountability. It is therefore essential to ensure that, in carrying out its investigations, fundamental rights including the rights to data protection and privacy of the persons implicated therein are properly guaranteed.

### 1.3. Main elements of the Proposal

9. The stated aim of the Proposal is to increase the efficiency, effectiveness and accountability of OLAF, while safeguarding its investigative independence. This purpose would be achieved mainly by: (i) increasing the cooperation and information exchange with other EU institutions, offices, bodies and agencies as well as Member States; (ii) fine-tuning the *de minimis* approach <sup>(6)</sup> to investigations; (iii) strengthening the procedural guarantees for the persons under investigation by OLAF; (iv) including the possibility for OLAF to conclude administrative arrangements to facilitate information exchange with Europol, Eurojust, competent authorities of third countries as well as with international organisations and (v) clarifying the monitoring role of the Supervisory Committee.
10. The EDPS supports the objectives of the proposed amendments and, in this respect, welcomes the Proposal. The EDPS particularly appreciates the introduction of the new Article 7(a) which is dedicated to the procedural guarantees afforded to individuals. In relation to individuals' rights to the protection of their personal data and privacy, the EDPS considers that on the whole the Proposal contains improvements *vis-à-vis* the current situation. In particular, the EDPS welcomes the express

recognition of the importance of the rights of the data subjects pursuant to Article 11 and 12 of Regulation (EC) No 45/2001 <sup>(7)</sup>.

11. However, despite the overall positive impression, the EDPS considers that from the point of view of the protection of personal data, the Proposal could be further improved without jeopardising the objectives that it pursues. In particular, the EDPS is concerned that, because of the lack of coherence on certain aspects, the Proposal may be interpreted as a *lex specialis* regulating the processing of personal data collected in the scope of OLAF investigations, which would take precedence over the application of the general data protection framework contained in Regulation (EC) No 45/2001. Thus, there is a risk that the data protection standards contained in the Proposal could be interpreted *ex contrario* as being lower than those contained in the Regulation, and this is without any apparent justification neither in the Proposal itself nor the Explanatory Memorandum.
12. In order to avoid this outcome, the following sections provide an analysis of the Proposal which, on the one hand, describes its shortcomings and, on the other hand, suggests specific ways to improve upon them. The scope of this analysis is limited to the provisions having a direct impact on personal data protection, particularly Article 1, paragraphs (8), (9), (10), (11) and (12) pursuant to which Articles 7a, 7b, 8, 9 10 and 10a are added or amended.

## 2. ANALYSIS OF THE PROPOSAL

### 2.1. General context

13. OLAF was created in 1999 <sup>(8)</sup> to protect the EU's financial interests and taxpayers' money against fraud, corruption and any other illegal activity. The Office is attached to the Commission, but it is independent of it. OLAF conducts investigations, which can be external <sup>(9)</sup> (in particular, investigations which can take place in the Member States or in third countries) and internal <sup>(10)</sup> (investigations within the EU institutions, bodies, offices and agencies) with the purpose to fight fraud and illegal activity which might harm the financial interests of the European Union.
14. Furthermore, OLAF can also (i) forward to national competent authorities information uncovered during its external investigations; (ii) forward to the national judiciary bodies information found during internal

<sup>(7)</sup> See the Proposal, new Article 7(a) and 8(4).

<sup>(8)</sup> Commission Decision 1999/352/EC of 28 April 1999 establishing the European Anti-Fraud Office (OLAF), OJ L 136, 31.5.1999, p. 20. See also Regulation (EC) No 1073/1999 of the European Parliament and the Council of 25 May 1999 concerning investigation conducted by the European Anti-Fraud Office (OLAF), OJ L 136, 31.5.1999, p. 1.

<sup>(9)</sup> See Article 3, Regulation (EC) No 1073/1999.

<sup>(10)</sup> See Article 1 and 4, Regulation (EC) No 1073/1999.

<sup>(6)</sup> That is, OLAF should define and focus on its investigative priorities in order to efficiently use its resources.

investigations into matters liable to result in criminal proceedings and (iii) forward to the institution, body, office or agency concerned the information obtained during internal investigations <sup>(11)</sup>.

15. OLAF can also closely cooperate with Eurojust <sup>(12)</sup> and Europol <sup>(13)</sup> to carry out its statutory duty to fight against fraud, corruption and any other activity which might affect the financial interest of the Union. In this context, Europol <sup>(14)</sup> and Eurojust <sup>(15)</sup> can exchange operational, strategic or technical information with OLAF, including personal data.
16. On the basis of Regulation (EC) No 1073/1999, OLAF can also investigate in third countries in accordance with the various cooperation agreements in force between the European Union and these third countries. Fraudulent activities to the detriment of the Union budget may also take place outside the territory of the European Union, for example with respect to foreign aid granted by the European Union to developing countries, candidate countries or other recipient countries, or with regard to

violations of customs legislation. In order to effectively detect and tackle these infringements, thus, OLAF needs to carry out on-the-spot inspections and checks in third countries as well. To illustrate the importance of international cooperation and, thus, also of data exchange, currently the European Union has more than 50 agreements on mutual administrative assistance in customs matters, including with large trading partners such as China, the United States of America, Japan, Turkey, the Russian Federation and India.

17. The implementation of Regulation (EC) No 45/2001 in the activities of OLAF has been the object of a number of interventions by the EDPS in the recent years. In relation to the focus of the Proposal (OLAF investigations), it is worth noting the Opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations <sup>(16)</sup>; Opinion of 4 October 2007 on five notifications for prior checking on external investigations <sup>(17)</sup> and the Opinion of 19 July 2007 on a notification for prior checking on regular monitoring of the implementation of the investigative function <sup>(18)</sup>, which relates to the activities of the Supervisory Committee.

<sup>(11)</sup> See Article 10, Regulation (EC) No 1073/1999.

<sup>(12)</sup> Eurojust was set up by Council Decision 2002/187/JHA (subsequently amended by Council Decision 2003/659/JHA, and Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust) as a body of the European Union with legal personality to stimulate and to improve coordination and cooperation between competent judicial authorities of the Member States. In particular, Article 26.4 of such decision established that 'OLAF may contribute to Eurojust's work to coordinate investigations and prosecution procedures regarding the protection of the financial interests of the Communities, either on the initiative of Eurojust or at the request of OLAF where the competent national authorities concerned do not oppose such participation'. In 2008, Eurojust and OLAF concluded an administrative agreement (Practical agreement on arrangements of cooperation between Eurojust and OLAF of 24 September 2008) which is aimed at enhancing the cooperation between the two entities and includes specific provision on the transfer of personal data.

<sup>(13)</sup> Europol is the European Law Enforcement Agency which aims at improving the effectiveness and cooperation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of organised crime. Article 22 of Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA) provides that 'In so far as it is relevant to the performance of its tasks, Europol may establish and maintain cooperative relations with [...] OLAF'. The article also provides that Europol can, before the entry into force of agreements or working arrangements with the various EU entities with which Europol is called to cooperate, 'directly receive and use information, including personal data from the entities [...] in so far as that is necessary for the legitimate performance of its tasks, and it may [...] directly transmit information, including personal data, to such entities, in so far as that is necessary for the legitimate performance of the recipient's task.'

<sup>(14)</sup> See Article 22 of Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ L 121, 15.5.2009, p. 37.

<sup>(15)</sup> See Article 1(26) of Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA.

## 2.2. Privacy and impact assessment

18. Neither the Proposal nor the Explanatory memorandum attached to it refers to the impact of the Proposal on the data protection rules. Nor does it refer to a privacy and data protection impact assessment. An explanation of how the impact on data protection has been dealt with would certainly increase the transparency of the overall assessment of the Proposal. The EDPS is surprised that the Explanatory Memorandum completely lacks any chapter on 'Results of consultations with the interested parties and impact assessments'.

## 2.3. Application of Regulation (EC) No 45/2001

19. As mentioned in the previous Opinion on the 2006 proposal <sup>(19)</sup>, the EDPS welcomes the Proposal's recognition that Regulation (EC) No 45/2001 applies to all data processing activities carried out by OLAF. In

<sup>(16)</sup> Case 2005-418 (<http://www.edps.europa.eu>).

<sup>(17)</sup> Cases 2007-47, 2007-48, 2007-49, 2007-50, 2007-72 (<http://www.edps.europa.eu>).

<sup>(18)</sup> Case 2007-73 (<http://www.edps.europa.eu>).

<sup>(19)</sup> EDPS Opinion on the Proposal for a Regulation of the European Parliament and the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ C 91, 26.4.2007, p. 1.

particular, the new formulation of Article 8(4) <sup>(20)</sup> clearly mentions the role of the Regulation in the context of OLAF's various activities. This constitutes an update of the text of Regulation (EC) No 1073/1999, which only mentioned Directive 95/46/EC as a reference for the data protection obligations.

20. The last sentence of Article 8(4) introduces the implementation of the requirement to appoint a data protection officer: 'The Office shall appoint a Data Protection Officer in accordance with Article 24 of Regulation (EC) No 45/2001'. This insertion, which formalises the actual appointment of the OLAF DPO, is also welcomed by the EDPS.

21. However, the EDPS is concerned that the implementation of the data protection standards in the proposed text is not completely in conformity with the requirements of the Regulation, and this might raise concerns as regards its coherence. This aspect will be analysed in detail below.

### 3. SPECIFIC COMMENTS

#### 3.1. OLAF and the respect of fundamental rights, including data protection principles

22. OLAF investigations can have a serious impact on the fundamental rights of individuals. As indicated by the Court of Justice in the *Kadi* judgment <sup>(21)</sup>, these rights are protected by the Community legal order. More precisely, in the *Schecke* judgment <sup>(22)</sup>, the Court, by reference to the Charter of Fundamental Rights of the European Union (Charter) <sup>(23)</sup>, and in particular to Articles 8 and 52 thereof, highlights that any limitation to the right to the protection of personal data can be justified only if it is

provided by law, if it respects the essence of the right, and if it is subject to proportionality and meets the objectives of general interest of the European Union. The EDPS places great weight on the respect of fundamental rights in the area of activity of OLAF.

23. Recital 13 of the Proposal clarifies that the fundamental rights of the persons concerned by an investigation should be respected at all times, and in particular when information about ongoing investigations is provided. The recital then highlights the need to respect confidentiality of investigations, the legitimate rights of the persons concerned, the national provisions governing judicial proceedings and, ultimately, the Union's legislation on data protection. It is specified that the exchange of information should be governed by the proportionality and need-to-know principles.

24. This recital seems to introduce a limitation to the applicability of fundamental rights both *ratione personae* (limited to persons concerned by the investigation) and *ratione materiae* (limited to exchange of information). This could lead to a incorrect interpretation of the text according to which fundamental rights in the area of OLAF's activities would be applied in a 'restrictive' way <sup>(24)</sup>.

25. The EDPS therefore suggests modifying the text of the recital in order to avoid possible misinterpretations: the recital mentions that the fundamental rights of 'persons concerned by an investigation' should be respected at all times. As OLAF not only deals with persons concerned by an investigation (suspects) but also with informants (persons providing information about the fact of a possible or actual case), whistleblowers <sup>(25)</sup> (persons within the EU institutions who report to OLAF facts related to a possible or actual case), and witnesses, the provision should more broadly define the categories of 'persons' who enjoy the fundamental rights.

26. Furthermore, recital 13 concerns respect for fundamental rights in particular in the context of the 'exchange of information'. The recital mentions, besides fundamental rights and confidentiality, that 'Information forwarded or obtained during investigations should be treated in accordance with the Union legislation on data protection'. The location of this sentence might be confusing and it should be placed in a separate recital to clarify that respect for data protection legislation is separate and self-standing and is not only related to exchange of information.

<sup>(20)</sup> The Office shall process only such personal data as necessary to fulfil its tasks under this Regulation. Such processing of personal data shall be done in conformity with Regulation (EC) No 45/2001, including the provision of relevant information to the data subject required by Articles 11 and 12 of that Regulation. Such information may not be communicated to persons other than those within the institutions of the Union or in the Member States whose functions require them to know, nor may it be used for purposes other than to prevent fraud, corruption or any other illegal activity. (...).

<sup>(21)</sup> Judgment of 3 September 2008 in joined Cases C-402/05 P and C-415/05 P, *Kadi v Council of the European Union and Commission of the European Communities*, para 283: '[...] fundamental rights form an integral part of the general principles of law whose observance the Court ensures. For that purpose, the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which they are signatories. In that regard, the ECHR has special significance.' See also paragraph 304.

<sup>(22)</sup> Judgment of 9 November 2010 in joined cases C-92/09 and C-93/09, *Volker und Markus Schecke*, paragraph 44 *et seq.*

<sup>(23)</sup> After the entry into force of the Lisbon Treaty, the ECHR is applicable to all areas of activity of the European Union.

<sup>(24)</sup> See also paragraph 36 below.

<sup>(25)</sup> See Opinion on a notification for prior-checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations, 23 June 2006, Case 2005/0418 (<http://www.edps.europa.eu>).

27. The EDPS welcomes the fact that Article 7(a) is specifically dedicated to procedural guarantees during investigations. This new provision is in line with the stated purpose of the Proposal to reinforce the accountability of OLAF. The Article also refers to the Charter, which includes provisions that are relevant in relation to OLAF's investigations, namely Article 8 (Protection of personal data) and the entire Chapter VI (Justice).
28. Article 7(a)(1) of the Proposal requires the Office to seek evidence for and against the person concerned, and recalls the duty to carry out investigations objectively and impartially. These principles have a positive impact on the 'data quality' <sup>(26)</sup> principle established in Article 4 of Regulation (EC) No 45/2001, in as much as the criterion requires the data to be accurate, conform to objective reality and be complete and up-to-date. The EDPS therefore welcomes the insertion of this paragraph.

*Right of information, access and rectification*

29. The following paragraphs of Article 7(a) concern the different steps of OLAF's investigations. These steps can be summarised as follows: (i) interviews with witnesses or persons concerned (paragraph 7(a)(2)); (ii) person found to be concerned by the investigations (paragraph 7(a)(3)); (iii) conclusions of the investigation referring to the name of a person (paragraph 7(a)(4)).
30. The EDPS notes that the obligation to provide the information pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001 is mentioned (only) in relation to step (iii) above. The EDPS is pleased that the Proposal has integrated the EDPS' recommendations provided in his legislative Opinion of 2006 <sup>(27)</sup>.
31. However, such a selective mentioning of the rights of the data subject in relation to a single procedural stage may be interpreted in a way that the same information should not be granted to the data subject (witness or person concerned) when he or she is invited to an interview or when the staff member is informed that he or she may be concerned by the investigation. For reasons of legal certainty, the EDPS therefore suggests that the reference to the relevant articles should be inserted in relation to all of the three situations mentioned in points (i), (ii) and (iii) above. However, once the information related to

Article 11 or 12 of Regulation (EC) No 45/2001 has been provided to the data subject, it will not be necessary to provide the same information in the following steps.

32. Furthermore, the text does not introduce any specification as regards the data subjects' rights of access and rectification of the data pursuant to Articles 13 and 14 of Regulation (EC) No 45/2001. These rights are protected by Article 8(2) of the Charter and therefore have a special prominence among the rights of the data subject. The EDPS had already asked <sup>(28)</sup> for the insertion of a clearer specification of the rights of access and rectification of the data subject in order to avoid the risk of interpreting the text as introducing a special 'lower standard' data protection regime for the persons concerned by OLAF investigations. The EDPS regrets that these aspects are not addressed in the Proposal.
33. The EDPS would also like to point out the possibility to limit the rights of information, access and rectification in specific cases, as provided for by Article 20 of Regulation (EC) No 45/2001. OLAF's compliance with the data protection rules can therefore coexist with the necessity to preserve the confidentiality of its investigations. This aspect will be further developed in the paragraphs below.

*Confidentiality of the investigation and rights of the data subject*

34. As a general remark, the EDPS acknowledges that the investigative role of OLAF requires the ability to protect the confidentiality of its investigations with the purpose of effectively tackling the fraud and illicit activities that it is required to pursue. The EDPS however highlights that this ability has an impact on certain rights of data subjects, and that Regulation (EC) No 45/2001 establishes specific conditions under which such rights can be restricted in this context (Article 20).
35. According to Article 20 of Regulation (EC) No 45/2001, the rights provided by Articles 4 (data quality) and 11 to 17 (information to be supplied, right of access, rectification, blocking, erasure, right to obtain notification to third parties) can be restricted so long as this is necessary to safeguard, among others: '(a) the prevention, investigation, detection and prosecution of criminal offences' or '(b) economic and financial interests of Member States or of the European Communities' and '(d) a monitoring, inspection [...] task connected with the exercise of official authority in cases referred to in points (a) and (b) above'. The same Article provides that the principal reasons why a restriction is imposed should be communicated to the data subject and that the subject should be made aware of the possibility to have recourse to the EDPS (Article 20(3)). Furthermore, Article 20(5) provides that such communication may be deferred for as long as providing the information to the data subject would deprive the restriction imposed of its effect.

<sup>(26)</sup> See footnote 25.

<sup>(27)</sup> Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ C 91, 26.4.2007, p. 1, paragraph 14 *et seq.*

<sup>(28)</sup> In its Opinion of 2006, see footnote 19 above.



36. The text of the Proposal essentially introduces exceptions to the rights of data subjects for reasons of confidentiality of the investigations. Article 7(a)(4) provides that 'Without prejudice to Articles 4(6) and 6(5)' <sup>(29)</sup>, no conclusions referring by name to a person concerned may be drawn 'once the investigation has been completed without that person being given the opportunity to comment on facts concerning him or her in writing or at an interview [...] and being provided with the information required by Articles 11 and 12 of Regulation No 45/2001'. The text seems therefore to suggest that, in the cases provided by Articles 4(6) and 6(5), the right to be heard and the right to information of the data subject could be limited.
37. The Proposal further establishes that, if necessary to preserve the confidentiality of the investigations and in cases entailing the use of investigations falling within the remit of a national judicial authority, the Director-General of OLAF may decide to defer the possibility for the person to make her or his view known. The text does not specify whether in this context also the information required by Articles 11 and 12 of Regulation (EC) No 45/2001 should be deferred.
38. The formulation of the text is unclear. First, the connection between the possible limitations of the rights of the person under investigation in relation to conclusions connected to his/her name and the type of information that OLAF should communicate to the relevant EU entity in the actual investigation are far from clear. Second, it is not clear which categories of the rights of the data subject are the object of a potential restriction. Third, the Article fails to insert the necessary safeguard of Article 20(3) of Regulation (EC) No 45/2001.
39. The consequence could be that individuals in some cases could be faced with conclusions on the investigation without having been aware of being subject to the investigation and without receiving any information on the reasons why their rights to be heard and rights of information pursuant to Articles 11 and 12 of Regulation (EC) 45/2001 have been restricted.
40. If Articles 20(3) and (5) of Regulation (EC) No 45/2001 are respected such a scenario would not be per se in conflict with the Regulation. However, the absence of a clear reference to the articles of the Regulation in the text does not appear to be consistent with the purpose of the Proposal to reinforce the procedural guarantees in favour of persons concerned by OLAF investigations and to enhance OLAF's accountability.
41. The EDPS therefore suggests that a possible limitation of the right of the data subject within the meaning of Article 20 of Regulation (EC) No 45/2001 should be introduced explicitly. In addition, the procedural safeguards of Article 20(3) should be mentioned in the text, as well as the possible exception of Article 20(5). Such a clear provision would enhance the legal certainty for the data subject and the accountability of OLAF.
42. In conclusion, in order to establish a clear set of rights for the data subject and to introduce possible exceptions due to confidentiality of the investigations compliant with Article 20 of Regulation (EC) No 45/2001, the EDPS suggests that the text should clearly indicate:
- the information to be supplied to the data subject in order to comply with data protection legislation (Articles 11 and 12 of Regulation (EC) No 45/2001) in the context of the various steps of OLAF's investigations <sup>(30)</sup>: (i) interviews (paragraph 7(a)(2)); (ii) provision of information when a person may be concerned by the investigation (paragraph 7(a)(3)) and (iii) at the end of the investigation (paragraph 7(a)(4));
  - the type of information that could be deferred by OLAF for reasons of confidentiality of the investigation, establishing clearly the conditions and the categories of data subjects concerned by the deferral;
  - the information that should be supplied to the data subject in order to comply with data protection legislation in case the communication pursuant to Article 11 or 12 is deferred or if the rights of access and rectification are limited (namely, the information pursuant to Article 20(3) of Regulation (EC) No 45/2001), including the exception related to the possibility to further defer the information pursuant to Article 20(5) of Regulation (EC) No 45/2001.
- <sup>(29)</sup> Article 4(6) — 'Internal investigation' — reads as follows: 'Where investigations reveal that a member or staff member may be concerned by an internal investigation, the institution, body, office or agency to which he belongs shall be informed. In exceptional cases where the confidentiality of the investigation cannot be ensured, the Office shall use appropriate alternative channels of information'. Article 6(5) — 'Investigations procedure' — reads as follows: 'Where investigations show that it might be appropriate to take precautionary administrative measures to protect the financial interests of the Union, the Office shall, without undue delay, inform the institution, body, office or agency concerned of the investigation in progress. The information supplied shall include the following: (a) the identity of any member or staff member concerned and a summary of the facts in question; (b) any information that may assist the institution, body, office or agency in deciding whether it is appropriate to take precautionary administrative measures in order to protect the financial interests of the Union; (c) any special measures of confidentiality recommended in particular in cases entailing the use of investigative measures falling under the competence of a national judicial authority or, in the case of an external investigation, under the competence of a national authority, in accordance with the national provisions applicable to investigations. [...]', emphasis added.
- <sup>(30)</sup> As mentioned above, once the information has been provided to the data subject, it would not be necessary to repeat the same information in the following steps.



### 3.2. Information policy

43. The EDPS highlights that any information on investigations which might be made public by OLAF can involve sensitive personal data, and the necessity of any such publication must be carefully evaluated. The Court of First Instance (now the General Court), in its judgment in the *Nikolaou* case in 2007 <sup>(31)</sup>, ruled that OLAF had violated Article 8(3) of Regulation (EC) No 1073/1999 <sup>(32)</sup> and Regulation (EC) No 45/2001 by not properly enforcing its obligation to ensure the protection of personal data in the context of a 'leak' <sup>(33)</sup> and of a publication of a press release <sup>(34)</sup>.
44. Therefore, the EDPS welcomes the introduction of paragraph 8(5) which provides explicitly that the Director-General shall ensure that information to the public is given 'neutrally, impartially' and in accordance with the principles set out in Article 8 and in Article 7(a). In the light of the comments made above on Article 7(a) in relation to its restrictive approach to the rules of Regulation (EC) No 45/2001, the EDPS particularly welcomes the reference in paragraph 8(5) to the more general provision of Article 8, which implies that any processing of personal data in the context of information to the public shall be done in conformity with all the principles Regulation (EC) No 45/2001.

### 3.3. Confidentiality of the identity of whistleblowers and informants

45. The EDPS would like to insist, in the context of the current revision, on the need to introduce a specific provision to guarantee the confidentiality of whistleblowers' and informants' identity. The EDPS underlines that the position of whistleblowers is a sensitive one. Persons that provide such information should be guaranteed that their identity is kept confidential, in particular vis-à-vis the person about whom an alleged wrongdoing is being reported <sup>(35)</sup>. The present guarantees (Commission

Communication SEC/2004/151/2) do not appear to be sufficient from a legal point of view. The EDPS notes that such provision would be in line with the Opinion of the Article 29 Data Protection Working Party on internal whistleblowing schemes <sup>(36)</sup>.

46. The EDPS recommends amending the current Proposal and ensuring that the identity of whistleblowers and informants is kept confidential during the investigations so long as this does not contravene national rules regulating judicial procedures. In particular, the subject of the allegations might be entitled to know the identity of the whistleblower and/or informant to instigate legal procedures against them if it has been established that they maliciously made false statements about him/her <sup>(37)</sup>.

### 3.4. Transfers of personal data from OLAF

#### *Cooperation with Eurojust and Europol*

47. The EDPS welcomes the specifications made in recital 6 and Article 10(a), and in particular the introduction of the requirement for a clear legal basis governing the co-operation with Eurojust and Europol, which is fully in line with Regulation (EC) No 45/2001. However, the Proposal should be more detailed in order to reflect the different data protection regimes for Eurojust and Europol.

48. To date, OLAF has in place a Practical Agreement with Eurojust <sup>(38)</sup> which spells out the conditions under which the transfer of personal data can take place. The co-operation between OLAF and Eurojust includes in particular the exchange of case summaries, of case-related strategic and operational information, the participation to meetings and the mutual assistance that may be useful for the efficient and effective fulfilment of their respective tasks. The Practical Agreement <sup>(39)</sup> mostly defines the *modus operandi* for the exchange of information, including personal data, and in some cases also highlights or specifies certain elements of the existing legal framework.

<sup>(31)</sup> Case T-259/03, *Nikolaou v Commission*, 12 July 2007, OJ C 247, 20.10.2007, p. 23.

<sup>(32)</sup> The article specifically refers to data protection law.

<sup>(33)</sup> *Nikolaou*, paragraph 213.

<sup>(34)</sup> *Nikolaou*, paragraph 232.

<sup>(35)</sup> 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).

<sup>(36)</sup> See Opinion 1/2006 of the Article 29 Working Party of 1 February 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 ([http://ec.europa.eu/justice/policies/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm)).

<sup>(37)</sup> See opinion on financial rules applicable to the annual budget of the Union 15 April 2011 (<http://www.edps.europa.eu>).

<sup>(38)</sup> Practical agreement on arrangements of cooperation between Eurojust and OLAF of 24 September 2008: see footnote above.

<sup>(39)</sup> Eurojust-OLAF Practical agreement, point 4.1.

49. As regards Europol, such an agreement is not in place with OLAF<sup>(40)</sup>, but the Europol decision permits Europol to directly receive, use and transmit information, including personal data, from, inter alia, OLAF also before the conclusion of a formal exchange agreement as long as this is necessary for the legitimate performance of Europol's and OLAF's tasks<sup>(41)</sup>. The exchange is also subject to the existence of a confidentiality agreement between the two entities. Article 24 of the Europol Decision specifies some safeguards that Europol should observe in relation to any data transfer which takes place before the conclusion of a formal exchange agreement: 'Europol shall be responsible for the legality of the transmission of data. Europol shall keep a record of all transmissions of data under this Article and of the grounds for such transmissions. Data shall be transmitted only if the recipient gives an undertaking that the data will be used only for the purpose for which they were transmitted'. Article 29 of the same decision also specifies when the responsibility for the data transferred by third parties falls on Europol.

50. The conclusion of a specific agreement with Europol on data transfers is strongly supported by the EDPS, and the fact that so far it has not been concluded reinforces the need for specific guarantees in the text of the Proposal. In view of the different data protection regimes in relation to the transfer of personal data from OLAF to Eurojust and Europol and vice versa, the EDPS believes that the Proposal should address more clearly the necessary guarantees and standards which should govern the cooperation between OLAF and those bodies and be taken into account in the current and future working arrangements between them.

51. In order to reinforce the need for the conclusion of an administrative arrangement, the provision of Article 10(a)(2) should be changed to read 'The Office shall agree on administrative arrangements [...]'. This way, it would mirror the similar provision of the Europol decision<sup>(42)</sup>, which establishes that Europol shall conclude agreements or working arrangements with other Union institutions, bodies and agencies. Furthermore, the Proposal could clarify in Article 10(a) that, as a general principle, the exchange of personal data with Eurojust and Europol should be limited to and should not exceed what is necessary for the legitimate performance of the tasks entrusted to OLAF, Europol and Eurojust. The Proposal should also introduce the obligation for OLAF to keep a record of all transmissions of data and the grounds of such transmissions, in order to reinforce the accountability of

OLAF as to the implementation of the obligations imposed by Regulation (EC) No 45/2001 on transfers of personal data.

#### *Cooperation with third countries and international organisations*

52. Paragraph 3 of Article 10(a) mentions that 'The Office may [also] agree, as appropriate, on administrative arrangements with competent services in third countries and international organisations. The Office shall coordinate with the Commission services concerned and the European External Action Service'.

53. The EDPS welcomes the fact that the cooperation of OLAF with third countries and international organisations is connected to the conclusion of administrative arrangements. However, the data protection implications resulting from the possible exchange of data with third countries and international organisations should be more specifically addressed in the Proposal.

54. The Proposal should be more precise on the specific requirements and conditions for possible transfers of data from and to third countries and organisations. The EDPS advises that the text of Article 10(a)(3) should include also the following wording: 'To the extent that cooperation with international organisations and third countries entails the transfer of personal data from OLAF to other entities, any such transfer should take place according to the criteria of Article 9 of Regulation (EC) No 45/2001'.

#### *Access by Supervisory Committee to personal data*

55. The EDPS welcomes the wording of Article 11 of the Proposal according to which 'The Supervisory Committee may ask the Office for additional information on investigations in duly justified situations, without however interfering with the conduct of investigations', since such wording expresses the principle of necessity in relation to any possible transfer of personal data from OLAF to the Supervisory Committee.

56. The issue of access of the Supervisory Committee to personal data of persons implicated or possibly implicated in investigations should also be clarified in the context of the rules of procedure to be adopted by the Committee on the basis of the new Article 11 paragraph 6. The EDPS would appreciate being involved in the process that would lead to the adoption of the rules of procedure of the Supervisory Committee. The consultation of the EDPS could also be inserted in the text of the Proposal as a requirement for the adoption of the rules of procedure.

<sup>(40)</sup> The Administrative Arrangement of 8 April 2004 is restricted to the exchange of strategic information and expressly excludes the exchange of personal data, leaving the issue to a further agreement between Europol and OLAF.

<sup>(41)</sup> Europol decision, Article 22.3, footnote 14 above.

<sup>(42)</sup> Europol decision, Article 22.2, see footnote 14 above: 'Europol shall conclude agreements of working arrangements with the entities referred to in paragraph 1' (namely, Eurojust, OLAF, Frontex, CEPOL, the ECB and the EMCDDA).

#### 4. STRATEGIC PLANNING

57. Besides all the specific points mentioned above, the EDPS would like to encourage the Commission to propose a more open approach to the EU data protection regime by OLAF. It would be the right moment for OLAF to develop a strategic planning of its data protection compliance by voluntarily clarifying the practical approach to the treatment of its numerous files containing personal data. OLAF could proactively and publicly explain how it treats personal data in its various activities. The EDPS believes that such a global and explicit approach would result in enhanced transparency of OLAF's treatment of personal data and in an ameliorated user friendliness of its investigative processes.
58. Therefore, the EDPS suggests that the provisions of the Proposal give the Director General the task of ensuring that a comprehensive overview of all different processing operations of OLAF is carried out and kept up to date, or that at least this is explained in a recital. Such an overview -the results of which should be transparent through, for example, an annual report or through other options- would not only enhance the effectiveness of the different activities of OLAF and their interaction, but also encourage OLAF to take a more global approach on the necessity and proportionality of processing operations. It would also be helpful to OLAF to better demonstrate that it properly implements privacy by design and accountability principles.

#### 5. CONCLUSION

59. In conclusion the EDPS welcomes those modifications introduced in the text which enhance the compliance of the Proposal with the EU data protection regime.
60. However, the EDPS would also like to highlight a number of shortcomings that should be addressed by the modification of the text, and most importantly:
- the Proposal should clearly mention the right to information of the different categories of data

subjects, as well as the right of access and rectification in relation to all the phases of the investigations carried out by OLAF;

- the Proposal should clarify the relationship between the need for confidentiality of the investigations and the data protection regime applicable during the investigations: the EDPS suggests that the rights of the data subjects should be clearly defined and separated as well as possible exceptions due to confidentiality requirements, and that the safeguards provided for by Article 20 of Regulation (EC) No 45/2001 should be explicitly introduced;
- the Proposal should clarify OLAF's information policy to the public in relation to data protection;
- the Proposal should introduce specific provisions for the confidentiality of whistleblowers and informants;
- the Proposal should clarify the general data protection principles on the basis of which OLAF can transmit and receive information, including personal data, with other EU bodies and agencies, third countries and international organisations;
- the provisions of the Proposal should give the Director-General the task of ensuring that a strategic and comprehensive overview of the different processing operations of OLAF is carried out, kept up to date and made transparent, or at least that the need for this should be explained in a recital.

Done at Brussels, 1 June 2011.

Giovanni BUTTARELLI  
Assistant European Data Protection Supervisor

**Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council on energy market integrity and transparency**

(2011/C 279/03)

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 <sup>(1)</sup>,

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 <sup>(2)</sup>, and in particular Article 41 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

**I. INTRODUCTION**

1. On 8 December 2010, the European Commission adopted a proposal for a Regulation of the European Parliament and of the Council on energy market integrity and transparency <sup>(3)</sup> ('Proposal').
2. The Commission did not consult the EDPS, although Article 28(2) of Regulation (EC) No 45/2001 would have required this. Acting on his own initiative, the EDPS adopts this Opinion based on Article 41(2) of this Regulation. The EDPS is aware that this advice comes at a late stage in the legislative process. Nevertheless, he finds it appropriate and useful to issue this Opinion, given the significant potential impact of the Proposal on the right to privacy and the protection of personal data. A reference to this Opinion should be included in the preamble of the Proposal.
3. The main aim of the Proposal is to prevent market manipulation and insider trading on wholesale energy (gas and electricity) markets. Market integrity and transparency of wholesale markets, where gas and electricity are traded between companies producing energy and traders, are key to the prices consumers finally pay.

4. To this end, the Proposal aims at establishing comprehensive rules at EU level to prevent traders from using inside information to their own benefit and from manipulating the market by artificially causing prices to be higher than would be justified by availability, production cost, capacity to store or to transport energy. In particular, the proposed rules prohibit the following:

- use of inside information when selling or buying energy at the wholesale market level; exclusive and price sensitive information should be disclosed before trading can take place,
- transactions that give false or misleading signals about the supply, demand or prices of wholesale energy market products, and
- distributing false news or rumours that give misleading signals about these products.

5. Market monitoring at the European level to uncover possible infringements of these prohibitions will be the responsibility of the European Agency for the Cooperation of Energy Regulators (the 'ACER') <sup>(4)</sup>.
6. Pursuant to the Proposal, the ACER will have timely access to information on the transactions taking place on wholesale energy markets. This includes information on price, quantity sold and the parties involved. This bulk data will also be shared with national regulators that will then be responsible for investigation of suspected abuses. In cases with a cross-border impact, the ACER will have the power to coordinate investigations. National regulatory authorities in Member States will enforce penalties.
7. The Proposal follows a number of other recent legislative proposals with a view to strengthening the existing financial supervisory arrangements and improving coordination and cooperation at EU level, including the Directive on insider dealing and market manipulation ('MAD') <sup>(5)</sup> and the Directive on markets in financial

<sup>(1)</sup> OJ L 281, 23.11.1995, p. 31 (hereinafter, 'Directive 95/46/EC').

<sup>(2)</sup> OJ L 8, 12.1.2001, p. 1 (hereinafter, 'Regulation (EC) No 45/2001').

<sup>(3)</sup> COM(2010) 726 final.

<sup>(4)</sup> ACER is a European Union body established in 2010. Its mission is to assist national energy regulatory authorities in exercising, at EU level, the regulatory tasks that they perform in the Member States and, where necessary, to coordinate their action.

<sup>(5)</sup> 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.



instruments ('MiFID') <sup>(1)</sup>. The EDPS recently commented on another one of these recent proposals <sup>(2)</sup>.

## II. EDPS COMMENTS AND RECOMMENDATIONS

8. The Proposal contains several provisions relevant to the protection of personal data:

- Articles 6 to 8 on market monitoring and reporting,
- Article 9 on 'data protection and operational reliability',
- Articles 10 and 11 on investigation and enforcement, and
- Article 14 on 'relations with third countries'.

### II.1. Market monitoring and reporting (Articles 6 to 8)

#### *Relevant provisions*

9. The Proposal is based on the premise that in order to detect market abuse (i) it is necessary to have an effectively functioning market monitoring system with timely access to complete transactional data; and that (ii) this should include monitoring at the EU level. Therefore, the proposed Regulation provides for the ACER to gather, review and share (with relevant national and EU authorities) a large amount of bulk data from wholesale energy markets.
10. In particular, the proposed Regulation requires market participants to provide the ACER with 'records of their transactions' in wholesale energy products. In addition to records of transactions, market participants are also required to provide the ACER with information related to the 'capacities of facilities for production, storage, consumption or transmission of electricity or natural gas'.
11. The form, content and timing of the information to be provided will be laid down in delegated acts of the Commission.

#### *EDPS comments and recommendations*

12. Considering that the Proposal leaves it entirely up to delegated acts to define the content of the information

which is to be collected in the framework of this monitoring and reporting exercise, it cannot be excluded that personal data — i.e. any information relating to an identified or identifiable natural person <sup>(3)</sup> — will be involved. Under current EU law this is only allowed, where necessary and proportionate in view of the specific purpose <sup>(4)</sup>. The proposed Regulation should therefore clearly specify whether and to what extent the records of transactions and capacity information to be collected for monitoring purposes may include any personal data <sup>(5)</sup>.

13. If the processing of personal data is foreseen, specific safeguards — for example, regarding purpose limitation, retention period and potential recipients of the information — may also be required. Considering their essential nature, these data protection safeguards should then be set forth directly in the text of the proposed Regulation rather than in delegated acts.

14. If, in contrast, no processing of personal data is expected (or such processing would only be exceptional and would be restricted to rare cases, where a wholesale energy trader might be an individual rather than a legal entity), this should be clearly set forth in the Proposal, at least in a recital.

### II.2. Data protection and operational reliability (Article 9)

#### *Relevant provisions*

15. Article 9(1) requires the ACER to 'ensure the confidentiality, integrity and protection' of the information it receives under Article 7 (i.e. records of transactions and capacity information collected in the framework of the market monitoring exercise). Article 9 also provides that 'where relevant', the ACER 'will comply' with Regulation (EC) No 45/2001 when it processes personal data under Article 7.
16. Furthermore, Article 9(1) also requires the ACER to 'identify sources of operational risk and minimise them through the development of appropriate systems, controls and procedures'.

17. Finally, Article 9(2) allows the ACER to make public parts of the information that it holds, 'provided that commercially sensitive information on individual market participants or individual transactions is not released'.

<sup>(1)</sup> 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.

<sup>(2)</sup> For more on the broader context of related legislative proposals, see the EDPS Opinion on the proposal for a Regulation of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories, issued on 19 April 2011; in particular, paragraphs 4, 5, and 17-20.

<sup>(3)</sup> See Article 2(a) of Directive 95/46/EC and Article 2(a) of Regulation (EC) No 45/2001.

<sup>(4)</sup> See Articles 6(1)(c) and 7(c) of Directive 95/46/EC and Article 4(1)(c) and 5(b) of Regulation (EC) No 45/2001.

<sup>(5)</sup> Article 9(1) of the Proposal — referring to Regulation (EC) No 45/2001 — suggests that this may be the case, but does not provide any further details. See more on this in Section II.2 of this Opinion.

*EDPS comments and recommendations*

18. The EDPS welcomes the fact that Article 9 is dedicated, in part, to data protection, and that the proposed Regulation specifically requires the ACER to comply with Regulation (EC) No 45/2001.

(a) *Applicability of Regulation (EC) No 45/2001 and Directive 95/46/EC*

19. Having said that, the EDPS emphasises that Regulation (EC) No 45/2001 applies to the ACER in full by virtue of this Regulation whenever it processes personal data. Therefore, the Proposal should remind that Regulation (EC) No 45/2001 should apply to the ACER not only when it processes data under Article 7, but also in all other situations: importantly, also when the ACER processes personal data regarding suspected market abuse/infringements under Article 11. In addition, to be more precise, the EDPS recommends that instead of using the term 'where relevant' to describe situations where the ACER is required to comply with Regulation (EC) No 45/2001, the phrase 'whenever personal data are processed' is used.

20. Reference should also be made to Directive 95/46/EC considering that this Directive applies to processing of personal data by the national regulatory authorities involved. Indeed, for the sake of clarity, the EDPS recommends that the proposed Regulation should mention, in a general manner (at least in a recital), that while the ACER shall be subject to Regulation (EC) No 45/2001, Directive 95/46/EC shall apply to the national regulatory authorities concerned.

(b) *Accountability*

21. The EDPS welcomes the requirement that the ACER should identify and minimise operational risks through the development of appropriate systems, controls and procedures. To further strengthen the principle of accountability<sup>(1)</sup>, if the processing of personal data would play a structural role, the proposed Regulation should specifically require the ACER to establish a clear framework for accountability that ensures data protection compliance and provides evidence thereof. This clear framework established by the ACER should contain a number of elements, such as:

- adopting and updating, as necessary, a data protection policy on the basis of an impact assessment (to also include a security risk assessment). This data protection policy should also include a security plan,

- carrying out periodic audits to assess continued adequacy of and compliance with the data protection policy (including auditing the security plan),

- making public (at least partially) the results of these audits to reassure stakeholders with respect to data protection compliance, and

- notifying data breaches and other security incidents to the Commission DPO, affected data subjects, and when relevant to other stakeholders and authorities<sup>(2)</sup>.

22. Equivalent requirements should also apply to national regulatory authorities and other EU authorities concerned.

(c) *Publication of information by the ACER*

23. With regard to the requirement in Article 9(2) that the ACER should make public parts of the information, which it holds, the EDPS understands that the aim of this provision is not to authorise the ACER to publish data for purposes of 'naming and shaming' and to publicly disclose wrongdoings of companies or individuals.

24. With that said, the Proposal is silent on whether there is any intention to publicly disclose any personal data. Therefore, for the avoidance of any doubt, the proposed Regulation should either specifically provide that the published information should not contain any personal data or clarify what, if any, personal data may be disclosed.

25. If any personal data is to be published, the need for disclosure (e.g. for reasons of transparency) must be carefully considered and balanced against other competing concerns, such as the need to protect the rights to privacy and to the protection of personal data of the individuals concerned.

26. Accordingly, before any disclosure, a proportionality assessment should be carried out, taking into account the criteria established by the European Court of Justice in *Schecke*<sup>(3)</sup>. In this case the ECJ underlined that derogations and limitations in relation to the protection of personal data must apply only in so far as it is strictly necessary. The ECJ further considered that the European institutions should explore different methods of publication in order to

<sup>(1)</sup> See Section 7 of the EDPS Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union', issued on 14 January 2011 ([http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14\\_Personal\\_Data\\_Protection\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf)).

<sup>(2)</sup> See Section 6.3 of the EDPS Opinion of 14 January 2011 referred to above.

<sup>(3)</sup> ECJ judgment of 9 November 2010, joined Cases C-92/09 and C-93/09 (*Schecke and Eifert*); see, in particular, paragraphs 81, 65 and 86.

find the one which would be consistent with the purpose of the publication while causing the least interference with the data subjects' rights to private life and to the protection of personal data.

### II.3. Investigatory powers (Article 10)

#### *Relevant provisions*

27. The Proposal foresees that market monitoring will be followed by an investigation where market abuse is suspected and that this may lead to appropriate sanctions. Article 10(1), in particular, requires Member States to grant the national regulatory authorities the necessary investigative powers to ensure that the provisions of the Regulation on insider trading and market manipulation are applied <sup>(1)</sup>.

#### *EDPS comments and recommendations*

28. The EDPS welcomes the specification in Article 10(1) that (i) the investigatory powers shall be exercised (only) to ensure that the provisions of the Regulation on insider trading and market manipulation (Articles 3 and 4) are applied; and that (ii) these powers shall be exercised in a proportionate manner.
29. Having said that, the Proposal should go further to ensure legal certainty and an adequate level of protection for personal data. As it will be shown below, there are two main problems with the text of Article 10 as proposed. First, Article 10 does not designate sufficiently clearly the scope of the investigatory powers; for example, it is not sufficiently clear whether private telephone records may be required, or whether an on-site inspection may be carried out in a private home. Second, Article 10 also does not provide for the necessary procedural safeguards against the risk of unjustified intrusion into privacy or misuse of personal data; for example, it does not require a warrant from a judicial authority.
30. Both the scope of the investigatory powers and the necessary safeguards are presumably left for national law to specify. Indeed, Article 10(1) leaves many options open for Member States by providing that the investigatory powers 'may be exercised (a) directly; (b) in collaboration with other authorities or market undertakings; or (c) by application to the competent judicial authorities'. This appears to allow divergences in national practices, for example, as to whether and under what circumstances a warrant would be required from a judicial authority.
31. While some national laws may already provide for adequate procedural and data protection safeguards, in order to

ensure legal certainty to data subjects, certain clarifications should be made and certain minimum requirements with regard procedural and data protection safeguards should be set forth at the EU level, in the proposed Regulation, as will be discussed below.

32. As a general principle, the EDPS emphasises that when EU legislation requires Member States to take measures at the national level that have an effect on fundamental rights (such as the rights to privacy and to the protection of personal data), the legislation should also require effective measures to be taken simultaneously with the restrictive measures to ensure the protection of the fundamental rights at stake. In other words, harmonisation of potentially privacy-intrusive measures, such as investigatory powers, should be accompanied by harmonisation of adequate procedural and data protection safeguard based on best practice.
33. Such an approach may help prevent too wide divergences at the national level and ensure a higher and more uniform level of protection for personal data throughout the European Union.
34. If harmonisation of minimum safeguards at this stage is not feasible, at a minimum, the EDPS recommends that the proposed Regulation should specifically require the Member States to adopt national implementing measures to ensure the necessary procedural and data protection safeguards. This is all the more important as the chosen form of the legal instrument is a regulation, which is directly applicable, and, as a general rule, would not necessarily require further implementing measures in the Member States.

### II.4. On-site inspections (Article 10(2)(c))

#### *Relevant provisions*

35. The Proposal requires that the investigatory powers to be granted to national regulatory authorities specifically include the power to carry out on-site inspections (Article 10(2)(c)).

#### *EDPS comments and recommendations*

36. It is not clear whether these inspections would be limited to a business property (premises, land and vehicles) of a market participant or whether they may also be carried out in a private property (premises, land or vehicles) of individuals. It is equally unclear whether the inspections can also be carried out without prior warning ('dawn raids').
37. If the Commission envisages requiring Member States to authorise the regulatory authorities to carry out on-site inspections of private properties of individuals, or to carry out dawn raids, this should, first of all, be clearly specified.

<sup>(1)</sup> It is important to note that the proposed Regulation does not grant similar investigatory powers to the ACER. Such powers are also not foreseen for the ACER in Regulation (EC) No 713/2009 of the European Parliament and of the Council of 13 July 2009 establishing an Agency for the Cooperation of Energy Regulators, OJ L 211, 14.8.2009, p. 1.

38. Secondly, the EDPS also emphasises that the proportionality of on-site inspections on a private property (such as in private homes of individuals) is far from being self-evident and — if it is foreseen — should be specifically justified.
39. Thirdly, for this case additional safeguards would also be needed, particularly with regard to the conditions on which such inspections can be carried out. For example, and without limitation, the Proposal should specify that an on-site inspection can only be carried out in an individual's home if there is a reasonable and specific suspicion that evidence is stored in that particular home, which is relevant to prove a serious violation of Articles 3 or 4 of the Regulation (i.e. the provisions on prohibition of insider trading and market manipulation). Importantly, the Proposal should also require a judicial warrant in all Member States <sup>(1)</sup>.
40. Fourthly, to ensure proportionality and prevent excessive interference with private life, unannounced inspections in private homes should be subject to the additional condition that in the event of an announced visit, evidence would be likely to be destroyed or tampered with. This should be clearly foreseen in the proposed Regulation.

## II.5. Powers to require 'existing telephone and existing data traffic records' (Article 10(2)(d))

### Relevant provisions

41. Article 10(2)(d) requires that the powers of the national regulatory authorities should also specifically include the power to 'require existing telephone and existing data traffic records'.

### EDPS comments and recommendations

42. The EDPS acknowledges the value of telephone and data traffic records in insider trading cases, particularly in order to establish connections between insiders and traders. Having said that, the scope of this power is not sufficiently clear, neither are appropriate procedural and data protection safeguards foreseen. Therefore, the EDPS recommends that the Proposal should be clarified as discussed below. In particular, the following issues should be addressed:

#### (a) What type of telephone and data traffic records can be required?

43. For the sake of legal certainty, the Proposal should first of all clarify what types of records may, where necessary, be required by the authorities.
44. The Proposal should specifically limit the scope of the investigatory powers to (i) the contents of telephone,

e-mail and other data traffic records that are already routinely and lawfully collected by traders for business reasons to evidence transactions; and to (b) traffic data (e.g. who made the call or sent the information, to whom, and when) which are already available directly from the market participants (traders) concerned.

45. In addition, the Proposal should also specify that the records must have been collected for a lawful purpose and in compliance with applicable data protection laws, including provision of adequate information to data subjects under Articles 10 and 11 of Directive 95/46/EC.

#### (b) What does the qualification 'existing' refer to?

46. The EDPS welcomes the fact that the Proposal limits this power to 'existing' records and thus does not require the powers of the regulatory authorities to oblige a trader or third party to specifically intercept, monitor or record telephone or data traffic for the purposes of the investigation.

47. However, for the sake of avoidance of any doubt, this intention should be made clearer, at least in a recital. It should be avoided that there would be any room left for interpreting the proposed Regulation to give a legal basis for national regulatory authorities to intercept, monitor or record telephone or data communications, whether covertly or openly, with or without a warrant.

#### (c) Can content of telephone conversations and data traffic also be required or only traffic data?

48. The text of the Proposal refers to 'existing telephone and existing data traffic records'. It is not sufficiently clear whether both the contents of existing data and telephone communications and traffic data (e.g. who made the call or sent the information, to whom, and when) may be required.

49. This should be made clearer in the provisions of the proposed Regulation. As discussed in paragraphs 43 to 45, it should be clearly specified what type of records may be required, and it must be ensured that those records were collected in compliance with applicable data protection laws in the first place.

#### (d) Can records be required from Internet service providers and telecommunications companies?

50. The Proposal should unambiguously specify whom the national regulatory authorities can require records from. In this respect, the EDPS understands that Article 10(2)(d) is not intended to allow national authorities to require

<sup>(1)</sup> See, for example, the judgment of the European Court of Human Rights in *Funke v France* (Case No 82/1991/334/407), 25 February 1993, paragraphs 55 to 57.



traffic data from providers of 'publicly available electronic communications services' <sup>(1)</sup> (such as telephone companies or Internet service providers).

51. Indeed, the Proposal does not refer at all to such providers, and also does not use the term 'traffic data'. Importantly, it also does not refer to, either implicitly or explicitly, the fact that derogation would be sought from the requirements set out by the e-Privacy Directive <sup>(2)</sup>, which establishes the general principle that traffic data can be further processed only for the purpose of billing and interconnection payments.

52. For the sake of avoidance of any doubt, the EDPS recommends that the fact that the Proposal provides no legal basis for data to be required from providers of publicly available electronic communications services should be explicitly mentioned in the text of the proposed Regulation, at least in a recital.

(e) Can records be required from other third parties?

53. Further, the Proposal should clarify whether the national regulatory authorities may only require records from the market participant under investigation or whether they are also empowered to require records from third parties (such as from a party to a transaction with the market participant under investigation, or a hotel where an individual suspected of insider trading was staying) to provide their own records.

(f) Can any private records be required?

54. Finally, the Proposal should also clarify whether the authorities may also require private records of individuals, such as employees or executives of the market participant under investigation (e.g. text messages sent from personal mobile devices or browsing history of home Internet use stored on a home computer).

55. The proportionality of requiring private records is debatable and — if it is foreseen — should be specifically justified.

56. As with the case of on-site inspections (see paragraphs 35 to 40 above), the Proposal should require a warrant from a

judicial authority, as well as further specific safeguards if the authorities require any private records.

## II.6. Reporting of suspected market abuse (Article 11): purpose limitation and data retention

### *Relevant provisions*

57. With respect to cross-border cooperation, the ACER is given an important role, alerting national regulatory authorities of potential market abuse and facilitating information exchange. To facilitate cooperation, Article 11(2) also specifically requires national regulatory authorities to inform the ACER 'in as specific manner as possible' where they have reasonable grounds to suspect any breach of the proposed Regulation. In order to ensure a coordinated approach, Article 11(3) also requires information sharing among national regulatory authorities, competent financial authorities, the ACER, as well as the European Securities and Markets Authority (the 'ESMA') <sup>(3)</sup>.

### *EDPS comments and recommendations*

58. In accordance with the purpose limitation principle <sup>(4)</sup>, the Proposal should explicitly provide that any personal data transferred on the basis of Article 11 of the proposed Regulation (reports of suspected market abuse) should only be used for purposes of investigating the suspected market abuse reported. The information should in any case not be used for any purposes that are incompatible with that purpose.

59. Data should also not be retained for long periods of time. This is even more important in those cases, where it can be shown that the initial suspicion was unfounded. In those cases there needs to be a specific justification for further retention <sup>(5)</sup>.

60. In this respect, the Proposal should first set a maximum retention period for which the ACER and other recipients of the information may keep the data, taking into account the purposes of the data storage. Unless a suspected market abuse has led to a specific investigation and the investigation is still ongoing, all personal data related to reported suspected market abuse should be deleted from

<sup>(1)</sup> See Article 2(c) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications (Framework Directive), OJ L 108, 24.4.2002, p. 33.

<sup>(2)</sup> See Article 6(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

<sup>(3)</sup> ESMA is an independent EU authority that contributes to safeguarding the stability of the European Union's financial system by ensuring the integrity, transparency, efficiency and orderly functioning of securities markets, as well as enhancing investor protection.

<sup>(4)</sup> See Article 6(1)(b) of Directive 95/46/EC and Article 4(1)(b) of Regulation (EC) No 45/2001.

<sup>(5)</sup> By way of illustration, the EDPS mentions in this context the ruling of the European Court of Human Rights in the case of *S and Marper v the United Kingdom* (2008) (4 December 2008) (Application nos. 30562/04 and 30566/04), according to which the long-term retention of the data of persons not convicted of a criminal offence was a breach of their right to privacy under Article 8 of the European Convention on Human Rights.

the records of all recipients after the lapse of a specified period. Unless a longer retention period is clearly justified, the EDPS considers that deletion should be carried out at the latest two years following the date of reporting the suspicion <sup>(1)</sup>.

61. In the event that a suspicion proves to be unfounded and/or an investigation is closed without taking further action, the Proposal should oblige the reporting regulatory authority, the ACER, and any third party with access to information regarding suspected market abuse, to swiftly inform these parties so that they are able to update their own records accordingly (and/or delete the information regarding the reported suspicion from their records with immediate effect or after the lapse of a proportionate retention period as appropriate) <sup>(2)</sup>.
62. These provisions should help ensure that in cases where the suspicion has not been confirmed (or even investigated further), or where it has been established that a suspicion is unfounded, innocent individuals would not be kept on a 'black list' and 'under suspicion' for an unduly long period of time (see Article 6(e) of Directive 95/46/EC and corresponding Article 4(e) of Regulation (EC) No 45/2001).

## II.7. Data transfers to third countries (Article 14)

### *Relevant provisions*

63. Articles 7, 8 and 11 of the proposed Regulation provide for exchanges of data and information between the ACER, the ESMA and authorities of Member States. Article 14 ('Relations with third countries') provides that the ACER 'may enter into administrative arrangements with international organisations and the administrations of third countries'. This may lead to transfer of personal data from the ACER and possibly also from the ESMA and/or from the authorities of the Member States to international organisations and authorities of third countries.

### *EDPS comments and recommendations*

64. The EDPS recommends that Article 14 of the Proposal clarifies that transfers of personal data can only be made in accordance with Article 9 of Regulation (EC) No 45/2001 and Articles 25 and 26 of Directive 95/46/EC. In particular, international transfers shall only take place if the third country in question ensures an adequate level of protection, or to entities or individuals in a third country that does not afford adequate protection if the controller adduces adequate safeguards with respect

to the protection of the privacy and fundamental rights and freedoms of individuals and as regard the exercise of the corresponding rights.

65. The EDPS emphasises that derogations (such as those mentioned in Article 9(6) of Regulation (EC) No 45/2001 and 26(1) of Directive), should not be used, in principle, to justify mass, systematic and/or structural data transfers to third countries.

## II.8. Prior checking of the ACER's coordinative activities with regard to investigations

66. Some of the data shared among the ACER, the ESMA and various authorities in Member States regarding suspected infringements are likely to include personal data, such as the identity of the suspected perpetrators or other individuals involved (e.g. witnesses, whistle-blowers, employees or other individuals acting on behalf of the businesses involved in trading).
67. Article 27(1) of Regulation (EC) No 45/2001 provides that 'processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes shall be subject to prior checking by the European Data Protection Supervisor'. Article 27(2) specifically confirms that processing of data relating to 'suspected offences' and 'offences' presents such risks, and requires prior checking. Considering the role foreseen for the ACER in the coordination of investigations, it seems likely that it will process data relating to 'suspected offences' and thus, its activities will be subject to prior checking <sup>(3)</sup>.
68. In the framework of a prior checking procedure, the EDPS may provide the ACER with further guidance and specific recommendations with regard to compliance with data protection rules. Prior checking of the activities of ACER may also bring added value considering the fact that Regulation (EC) No 713/2009, which established the ACER, does not include any reference to the protection of personal data and has not been subject to a legislative opinion of the EDPS.

## III. CONCLUSIONS

69. The Proposal should clarify whether any personal data may be processed in the context of market monitoring and reporting and which safeguards will apply. If, in contrast, no processing of personal data is expected (or such processing would only be exceptional and would be restricted to rare cases, where a wholesale energy trader might be an individual rather than a legal entity), this should be clearly set forth in the Proposal, at least in a recital.

<sup>(1)</sup> Where a suspicion proves to be well-founded and leads to a successful investigation, the Proposal should set forth a specific — non-excessive — retention period following the closure of the investigation.

<sup>(2)</sup> This information should also be provided to the data subject concerned.

<sup>(3)</sup> It is to be noted that the data processing carried out by national authorities may also be subject to prior checking by national or regional data protection authorities under national data protection laws adopted pursuant to Article 20 of Directive 95/46/EC.

70. Provisions on data protection, data security and accountability should be clarified and further strengthened, especially if the processing of personal data would play a more structural role. The Commission should ensure that adequate controls are in place to ensure data protection compliance and provide evidence thereof ('accountability').
71. The Proposal should clarify whether on-site inspections would be limited to a business property (premises and vehicles) of a market participant or also apply to private properties (premises or vehicles) of individuals. In the latter case, the necessity and proportionality of this power should be clearly justified and a judicial warrant and additional safeguards should be required. This should be clearly foreseen in the proposed Regulation.
72. The scope of the powers to require 'existing telephone and existing data traffic records' should be clarified. The Proposal should unambiguously specify what records can be required and from whom. The fact that no data can be required from providers of publicly available electronic communications services should be explicitly mentioned in the text of the proposed Regulation, at least in a recital. The Proposal should also clarify whether the authorities may also require private records of individuals, such as employees or executives of the market participant under investigation (e.g. text messages sent from personal mobile devices or browsing history of home internet use). If this would be the case, the necessity and proportionality of this power should be clearly justified and the Proposal should also require a warrant from a judicial authority.
73. With regard to reporting of suspected market abuse, the Proposal should explicitly provide that any personal data contained in these reports should only be used for purposes of investigating the suspected market abuse reported. Unless a suspected market abuse has led to a specific investigation and the investigation is still ongoing (or a suspicion has proved to be well-founded and has led to a successful investigation), all personal data related to the reported suspected market abuse should be deleted from the records of all recipients after the lapse of a specified period (unless otherwise justified, at the latest two years following the date of report). In addition, parties to an information exchange should also send each other an update in case a suspicion proves to be unfounded and/or an investigation has been closed without taking further action.
74. With regard to transfers of personal data to third countries, the Proposal should clarify that in principle, transfers can only be made to entities or individuals in a third country that does not afford adequate protection if the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regard the exercise of the corresponding rights.
75. The ACER should submit to the EDPS for prior checking its personal data processing activities with regard to coordination of investigations under Article 11 of the proposed Regulation.

Done at Brussels, 21 June 2011.

Giovanni BUTTARELLI

*Assistant European Data Protection Supervisor*

## II

*(Information)*INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES  
AND AGENCIES

## EUROPEAN COMMISSION

**Non-opposition to a notified concentration****(Case COMP/M.6349 — Motherson/Cross Industries/Peguform/Wethje)****(Text with EEA relevance)**

(2011/C 279/04)

On 16 September 2011, the Commission decided not to oppose the above notified concentration and to declare it compatible with the common market. This decision is based on Article 6(1)(b) of Council Regulation (EC) No 139/2004. The full text of the decision is available only in English and will be made public after it is cleared of any business secrets it may contain. It will be available:

- in the merger section of the Competition website of the Commission (<http://ec.europa.eu/competition/mergers/cases/>). This website provides various facilities to help locate individual merger decisions, including company, case number, date and sectoral indexes,
- in electronic form on the EUR-Lex website (<http://eur-lex.europa.eu/en/index.htm>) under document number 32011M6349. EUR-Lex is the on-line access to the European law.

**Non-opposition to a notified concentration****(Case COMP/M.6218 — Ineos/Tessenderlo Group S-PVC Assets)****(Text with EEA relevance)**

(2011/C 279/05)

On 26 July 2011, the Commission decided not to oppose the above notified concentration and to declare it compatible with the common market. This decision is based on Article 6(1)(b) of Council Regulation (EC) No 139/2004. The full text of the decision is available only in English and will be made public after it is cleared of any business secrets it may contain. It will be available:

- in the merger section of the Competition website of the Commission (<http://ec.europa.eu/competition/mergers/cases/>). This website provides various facilities to help locate individual merger decisions, including company, case number, date and sectoral indexes,
- in electronic form on the EUR-Lex website (<http://eur-lex.europa.eu/en/index.htm>) under document number 32011M6218. EUR-Lex is the on-line access to the European law.



## IV

(Notices)

## NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

## EUROPEAN COMMISSION

**Euro exchange rates <sup>(1)</sup>****22 September 2011**

(2011/C 279/06)

**1 euro =**

| Currency |                  |         | Exchange rate |                       |           |
|----------|------------------|---------|---------------|-----------------------|-----------|
| Currency |                  |         | Exchange rate |                       |           |
| USD      | US dollar        | 1,3448  | AUD           | Australian dollar     | 1,3691    |
| JPY      | Japanese yen     | 102,59  | CAD           | Canadian dollar       | 1,3894    |
| DKK      | Danish krone     | 7,4458  | HKD           | Hong Kong dollar      | 10,4904   |
| GBP      | Pound sterling   | 0,87325 | NZD           | New Zealand dollar    | 1,7185    |
| SEK      | Swedish krona    | 9,2762  | SGD           | Singapore dollar      | 1,7547    |
| CHF      | Swiss franc      | 1,2275  | KRW           | South Korean won      | 1 605,66  |
| ISK      | Iceland króna    |         | ZAR           | South African rand    | 11,0754   |
| NOK      | Norwegian krone  | 7,8270  | CNY           | Chinese yuan renminbi | 8,6040    |
| BGN      | Bulgarian lev    | 1,9558  | HRK           | Croatian kuna         | 7,4845    |
| CZK      | Czech koruna     | 24,878  | IDR           | Indonesian rupiah     | 12 246,50 |
| HUF      | Hungarian forint | 293,06  | MYR           | Malaysian ringgit     | 4,2744    |
| LTL      | Lithuanian litas | 3,4528  | PHP           | Philippine peso       | 58,919    |
| LVL      | Latvian lats     | 0,7093  | RUB           | Russian rouble        | 43,2059   |
| PLN      | Polish zloty     | 4,4863  | THB           | Thai baht             | 41,379    |
| RON      | Romanian leu     | 4,3055  | BRL           | Brazilian real        | 2,4887    |
| TRY      | Turkish lira     | 2,4636  | MXN           | Mexican peso          | 18,6738   |
|          |                  |         | INR           | Indian rupee          | 66,6720   |

<sup>(1)</sup> Source: reference exchange rate published by the ECB.

## V

*(Announcements)*

## ADMINISTRATIVE PROCEDURES

## EUROPEAN COMMISSION

## MEDIA 2007 — DEVELOPMENT, DISTRIBUTION, PROMOTION AND TRAINING

## Call for proposals — EACEA/21/11

**Support for the development of production projects — Animation, creative documentaries and drama — Single Projects, Slate Funding and Slate Funding second stage**

(2011/C 279/07)

**1. Objectives and description**

This notice of a call for proposals is based on Decision No 1718/2006/EC of the European Parliament and of the Council of 15 November 2006 concerning the implementation of a programme of support for the European audiovisual sector (MEDIA 2007).

One of the objectives of the programme is to promote, by providing financial support, the development of production projects intended for European and international markets presented by independent European production companies in the following categories: animation, creative documentary and drama.

**2. Eligible applicants**

This notice is aimed at European companies whose activities contribute to the attainment of the above objectives, and in particular to independent production companies.

Applicants must be established in one of the following countries:

- the 27 countries of the European Union,
- the EEA countries, Croatia and Switzerland.

**3. Eligible actions**

The development activities for the following audiovisual works (one-offs or series) are eligible:

- drama projects intended for commercial exploitation of no less than 50 minutes,
- creative documentaries intended for commercial exploitation of no less than 25 minutes (duration per episode in case of series),
- animation projects intended for commercial exploitation of no less than 24 minutes.

The development and production activities for the following categories of work are ineligible:

- live recordings, TV games, talk shows, reality shows or educational, teaching and 'how-to' programmes,
- documentaries promoting tourism, 'making-of', reports, animal reportages, news programmes and 'docu-soaps',
- projects promoting, directly or indirectly, messages that are at odds with the policies of the European Union. For example, projects that may be contrary to the interests of public health (alcohol, tobacco, drugs), respect for human rights, people's security, freedom of expression etc.,
- projects promoting violence and/or racism and/or with a pornographic content,
- works of a promotional nature,
- institutional productions to promote a specific organisation or its activities.

The call for proposals 21/11 has two deadlines. To be included in the first deadline, the application for support must be sent to the Agency between the date of the publication of the call for proposals and 25 November 2011. To be included in the second deadline, the application for support must be sent to the Agency between 26 November 2011 and 13 April 2012, the date of closure of the call for proposals.

The maximum duration of the project is until 30 June 2014 for requests for support submitted within the first deadline and until 30 November 2014 for those requests submitted within the second deadline or until the date of entry into production of the project, whichever is the earliest.

#### **4. Award criteria**

Points will be allocated out of a total of 100 on the basis of the following weighting:

##### *For Single Project*

- Criteria relating to the applicant company (40 points):
  - quality of the development strategy (10),
  - consistency of the development budget (10),
  - quality of the financing strategy (10),
  - quality of the distribution strategy (10).
- Criteria relating to the submitted project (60 points):
  - quality of the project (40),
  - potential for production and the feasibility of the project (10),
  - potential for European and International distribution (10).

##### *For Slate Funding and Slate Funding second stage*

- Criteria relating to the applicant company (60 points):
  - capacity of the company to develop and produce at a European level (15 points for Slate Funding — 30 points for Slate Funding second stage),
  - quality of the development strategy and consistency of the development budget (15 points for Slate Funding — 10 points for Slate Funding second stage),

- quality of the financing strategy (15 points for Slate Funding — 10 points for Slate Funding second stage),
- quality of the distribution strategy (15 points for Slate Funding — 10 points for Slate Funding second stage).
- Criteria relating to the submitted projects (40 points):
  - quality of the projects (10),
  - potential of the creative team (10),
  - potential for production and the feasibility of the project (10),
  - potential for European and international distribution (10).

#### 5. Budget

The total budget available is EUR 17 million. The financial contribution awarded is a subsidy.

The maximum financial contribution which may be awarded for Single Project is between EUR 10 000 and EUR 60 000 except for feature-length animations for theatrical release, for which the maximum is EUR 80 000. The financial contribution awarded will in no event exceed 50 % of the eligible costs submitted by the producer (60 % for projects presenting an interest in promoting European cultural diversity).

The maximum financial contribution which may be awarded for Slate Funding and Slate Funding second stage is between EUR 70 000 and EUR 190 000. The financial contribution awarded will in no event exceed 50 % of the eligible costs submitted by the producer.

The Agency reserves the right not to distribute all the funds available.

#### 6. Deadline for submission of applications

Applications must be submitted to the Executive Agency (EACEA) using the online application form and the application package must be sent no later than **25 November 2011 and 13 April 2012** (see point 3) to the following address:

Education, Audiovisual and Culture Executive Agency (EACEA) — MEDIA  
Constantin DASKALAKIS  
BOUR 3/30  
Avenue du Bourget/Bourgetlaan 1  
1140 Bruxelles/Brussel  
BELGIQUE/BELGIË

Only applications submitted on the official application form, duly signed by the person entitled to enter into legally binding commitments on behalf of the applicant organisation will be accepted.

Applications sent by fax or email will be rejected.

#### 7. Full details

The full text of the guidelines together with the application forms can be found at the following Internet address: <http://www.ec.europa.eu/media>

Applications must comply with all the terms of the guidelines and be submitted on the forms provided.

---



**MEDIA 2007 — DEVELOPMENT, DISTRIBUTION, PROMOTION AND TRAINING****Call for proposals — EACEA/22/11****Support for the development of on- and off-line interactive works**

(2011/C 279/08)

**1. Objectives and description**

This notice of a call for proposals is based on Decision No 1718/2006/EC of the European Parliament and of the Council of 15 November 2006 concerning the implementation of a programme of support for the European audiovisual sector (MEDIA 2007).

One of the objectives of the programme is to promote, by providing financial support, the development of production projects intended for European and international markets presented by independent European production companies.

**2. Eligible applicants**

This notice is aimed at European companies whose activities contribute to the attainment of the above objectives, and in particular to independent production companies.

Applicants must be established in one of the following countries:

- the 27 countries of the European Union,
- the EEA countries, Croatia and Switzerland.

**3. Eligible actions**

The activities for the following interactive works are eligible:

The concept development (up to a first playable application) of digital interactive content complementing an audiovisual project (drama, creative documentary or animation) specifically developed for at least one of the following platforms:

- Internet,
- PC,
- console,
- handheld device,
- interactive television.

This digital content must present:

- substantial interactivity with a narrative component,
- originality, creativity and innovation against existing works,
- European commercial potential.

Only the following types of audiovisual project intended for commercial exploitation can be complemented by the submitted interactive work:

- a drama of at least 50 minutes (the total length of the series in the case of a series),

- a creative documentary of at least 25 minutes (length per episode in the case of a series),
- an animation of at least 24 minutes (the total length of the series in the case of a series).

The following activities are ineligible:

The development and production activities for the following categories of work are ineligible:

- reference works (encyclopaedias, atlases, catalogues, databases ...),
- 'how-to' works (education programmes, manuals ...),
- tools and software services,
- information services or purely transactional,
- information programs and magazines,
- projects promoting tourism,
- multimedia art projects,
- websites being, or dedicated specifically to, social platforms, social networking, Internet forums, blogs or similar activities,
- projects promoting, directly or indirectly, messages that are at odds with the policies of the European Union. For example, projects that may be contrary to the interests of public health (alcohol, tobacco, drugs), respect for human rights, people's security, freedom of expression, etc. are prohibited,
- projects promoting violence and/or racism and/or with a pornographic content,
- works of a promotional nature (in particular branded content),
- institutional productions to promote a specific organisation or its activities.

The call for proposals 22/11 has two deadlines. To be included in the first deadline, the application for support must be sent to the Agency between the date of the publication of the call for proposals and 25 November 2011. To be included in the second deadline, the application for support must be sent to the Agency between 26 November 2011 and 13 April 2012, the date of closure of the call for proposals.

The maximum duration of the project is until 30 June 2014 for requests for support submitted within the first deadline and until 30 November 2014 for those requests submitted within the second deadline or until the date of entry into production of the project, whichever is the earliest.

#### 4. Award criteria

Points will be allocated out of a total of 100 on the basis of the following weighting:

- Criteria relating to the applicant company (40 points):
  - quality of the development strategy (10),

- consistency of the development budget (10),
- capacity of the company to realise the project (10),
- quality of the financing strategy (10).
- Criteria relating to the submitted project (60 points):
  - quality of the content and originality of the concept against existing works (20),
  - innovation, appropriateness of the techniques used in the work and quality of interactivity (20),
  - potential for European exploitation and suitability for the target audience (20).

## 5. Budget

The total budget available is EUR 2,5 million. The financial contribution awarded is a subsidy.

The maximum financial contribution which may be awarded is between EUR 10 000 and EUR 150 000.

The financial contribution awarded will in no event exceed 50 % of the eligible costs submitted by the producer (60 % for projects presenting an interest in promoting European cultural diversity).

The Agency reserves the right not to distribute all the funds available.

## 6. Deadline for submission of applications

Applications must be submitted to the Executive Agency (EACEA) using the online application form and the application package must be sent no later than **25 November 2011 and 13 April 2012** (see point 3) to the following address:

Education, Audiovisual and Culture Executive Agency (EACEA) — MEDIA  
Constantin DASKALAKIS  
BOUR 3/30  
Avenue du Bourget/Bourgetlaan 1  
1140 Bruxelles/Brussel  
BELGIQUE/BELGIË

Only applications submitted on the official application form, duly signed by the person entitled to enter into legally binding commitments on behalf of the applicant organisation will be accepted.

Applications sent by fax or email will be rejected.

## 7. Full details

The full text of the guidelines together with the application forms can be found at the following Internet address:

<http://ec.europa.eu/media>

Applications must comply with all the terms of the guidelines and be submitted on the forms provided.

---

## PROCEDURES RELATING TO THE IMPLEMENTATION OF COMPETITION POLICY

### EUROPEAN COMMISSION

#### **Prior notification of a concentration**

**(Case COMP/M.6348 — Arla Foods/Allgäuland)**

**(Text with EEA relevance)**

(2011/C 279/09)

1. On 15 September 2011, the Commission received a notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 <sup>(1)</sup> by which the undertaking Hansa-Milch AG ('Hansa', Germany) belonging to Arla Foods Amba ('Arla', Denmark) acquires within the meaning of Article 3(1)(b) of the Merger Regulation control of the whole of Allgäuland-Käseereien GmbH and AL Dienstleistungs-GmbH (together referred to as 'Allgäuland', Germany) by way of purchase of shares.

2. The business activities of the undertakings concerned are:

- Arla is a dairy cooperative owned by dairy farmers. The company is active in the production and sale of a variety of dairy products. In Germany Arla is mainly active through its subsidiary Hansa,
- Allgäuland is a dairy cooperative and produces a variety of quality cheeses as well as other dairy products, mainly in Germany.

3. On preliminary examination, the Commission finds that the notified transaction could fall within the scope the EC Merger Regulation. However, the final decision on this point is reserved.

4. The Commission invites interested third parties to submit their possible observations on the proposed operation to the Commission.

Observations must reach the Commission not later than 10 days following the date of this publication. Observations can be sent to the Commission by fax (+32 22964301), by e-mail to COMP-MERGER-REGISTRY@ec.europa.eu or by post, under reference number COMP/M.6348 — Arla Foods/Allgäuland, to the following address:

European Commission  
Directorate-General for Competition  
Merger Registry  
J-70  
1049 Bruxelles/Brussel  
BELGIQUE/BELGIË

---

<sup>(1)</sup> OJ L 24, 29.1.2004, p. 1 (the 'EC Merger Regulation').

**Prior notification of a concentration**  
**(Case COMP/M.6392 — Gores/Mexx)**  
**Candidate case for simplified procedure**  
**(Text with EEA relevance)**  
(2011/C 279/10)

1. On 15 September 2011 the Commission received a notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 <sup>(1)</sup> by which the Gores Group LLC ('Gores', United States) acquire sole control over Mexx European Holding BV ('Mexx', Netherlands) within the meaning of Article 3(1)(b) of the Merger Regulation by way of purchase of shares.

2. The business activities of the undertakings concerned are:

- for Gores: private equity investor in technology, telecommunications, business services, industrial and apparel sectors primarily in the United States and Western Europe,
- for Mexx: retail of clothing, retail sale of footwear and accessories and wholesale of clothing and footwear in Europe and North America.

3. On preliminary examination, the Commission finds that the notified transaction could fall within the scope of the EC Merger Regulation. However, the final decision on this point is reserved. Pursuant to the Commission Notice on a simplified procedure for treatment of certain concentrations under the EC Merger Regulation <sup>(2)</sup> it should be noted that this case is a candidate for treatment under the procedure set out in the Notice.

4. The Commission invites interested third parties to submit their possible observations on the proposed operation to the Commission.

Observations must reach the Commission not later than 10 days following the date of this publication. Observations can be sent to the Commission by fax (+32 22964301), by e-mail to COMP-MERGER-REGISTRY@ec.europa.eu or by post, under reference number COMP/M.6392 — Gores/Mexx, to the following address:

European Commission  
Directorate-General for Competition  
Merger Registry  
J-70  
1049 Bruxelles/Brussel  
BELGIQUE/BELGIË

---

<sup>(1)</sup> OJ L 24, 29.1.2004, p. 1 (the 'EC Merger Regulation').

<sup>(2)</sup> OJ C 56, 5.3.2005, p. 32 ('Notice on a simplified procedure').











## 2011 SUBSCRIPTION PRICES (excluding VAT, including normal transport charges)

|                                                                                                                     |                                           |                    |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------|--------------------|
| EU Official Journal, L + C series, paper edition only                                                               | 22 official EU languages                  | EUR 1 100 per year |
| EU Official Journal, L + C series, paper + annual DVD                                                               | 22 official EU languages                  | EUR 1 200 per year |
| EU Official Journal, L series, paper edition only                                                                   | 22 official EU languages                  | EUR 770 per year   |
| EU Official Journal, L + C series, monthly DVD (cumulative)                                                         | 22 official EU languages                  | EUR 400 per year   |
| Supplement to the Official Journal (S series), tendering procedures for public contracts, DVD, one edition per week | multilingual:<br>23 official EU languages | EUR 300 per year   |
| EU Official Journal, C series — recruitment competitions                                                            | Language(s) according to competition(s)   | EUR 50 per year    |

Subscriptions to the *Official Journal of the European Union*, which is published in the official languages of the European Union, are available for 22 language versions. The Official Journal comprises two series, L (Legislation) and C (Information and Notices).

A separate subscription must be taken out for each language version.

In accordance with Council Regulation (EC) No 920/2005, published in Official Journal L 156 of 18 June 2005, the institutions of the European Union are temporarily not bound by the obligation to draft all acts in Irish and publish them in that language. Irish editions of the Official Journal are therefore sold separately.

Subscriptions to the Supplement to the Official Journal (S Series — tendering procedures for public contracts) cover all 23 official language versions on a single multilingual DVD.

On request, subscribers to the *Official Journal of the European Union* can receive the various Annexes to the Official Journal. Subscribers are informed of the publication of Annexes by notices inserted in the *Official Journal of the European Union*.

### Sales and subscriptions

Subscriptions to various priced periodicals, such as the subscription to the *Official Journal of the European Union*, are available from our sales agents. The list of sales agents is available at:

[http://publications.europa.eu/others/agents/index\\_en.htm](http://publications.europa.eu/others/agents/index_en.htm)

**EUR-Lex (<http://eur-lex.europa.eu>) offers direct access to European Union legislation free of charge. The *Official Journal of the European Union* can be consulted on this website, as can the Treaties, legislation, case-law and preparatory acts.**

**For further information on the European Union, see: <http://europa.eu>**



Publications Office of the European Union  
2985 Luxembourg  
LUXEMBOURG

EN