

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)

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 data¹,

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 sector²,

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 data³, 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').⁴ 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

¹ OJ 1995, L281/31.

² OJ 2002, L201/37 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ 2009, L337/11.

³ OJ 2001, L8/1.

⁴ COM(2011)225 final.

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.⁵ 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'.⁶

1.2. 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.
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) 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

⁵ The Data Retention Directive (Directive 2006/24/EC) was adopted on 15 March 2006 and published in OJ 2006, L105/54. The deadline for issuing the report was set at 15 September 2010, see Article 14(1) of the Data Retention Directive.

⁶ See p. 1 of the Evaluation report.

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

⁸ See ECHR 2 August 1984, *Malone v. UK*, A-82, para 84.

⁹ See the EDPS opinion of 26 September 2005, OJ 2005, C298/1. During a conference organised by the Commission in December 2010, the EDPS referred to the instrument as 'the most privacy invasive

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

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).

¹¹ See the EDPS opinion referred to in footnote 9.

¹² See furthermore Commission Decision of 25 March 2008, OJ 2008, L111/11.

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

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

¹⁵ In his opinion of 2005, the EDPS already emphasised the importance of the obligation to evaluate the instrument (see footnote 9, pts. 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.

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 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').¹⁹ 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 (Art. 3). It also includes data related to unsuccessful call attempts. No data revealing the content of communications may be retained pursuant to the Directive (Art. 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' (Art. 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.²⁰ The ePrivacy Directive requires that traffic and location data generated by using electronic communications services must be erased or made

¹⁹ See footnote 2.

²⁰ See Article 5 of the ePrivacy Directive.

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.²¹ 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.²²
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 Article 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.²³ 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.²⁴

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

²¹ See Articles 6 and 9 of the ePrivacy Directive.

²² See also the WP29 in the Report of 13 July 2010, referred to in footnote 13, p. 1.

²³ See p. 4 of the Evaluation report. See in this respect also Recital 12 of the Data Retention Directive.

²⁴ See the speech of 3 December 2010 referred to in footnote 9, p. 4.

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).²⁵

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.²⁶ 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.²⁷
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.²⁸
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.²⁹
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.³⁰ 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.

²⁵ A first proposal for EU rules on data retention (a framework decision) was based on the former EU Treaty, tabled by France, Ireland, 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.

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

²⁷ See ECJ 10 February 2009, *Ireland v. Parliament and Council*, C-301/06, para 82-83.

²⁸ See the opinion of 2005, pt. 80. See on this also part IV.3 of the present opinion.

²⁹ See p. 31 of the Evaluation report.

³⁰ See Article 6(1) TEU.

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'.³¹ The EDPS believes that the current evaluation process offers the Commission a good opportunity to give proof of this commitment.

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.³² 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'.³³ 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.³⁴ 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'.³⁵ However, in the opinion of 2005, the EDPS indicated not to be convinced by this statement, since it required further evidence.³⁶ 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

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

³² See p. 31 of the Evaluation report.

³³ See p. 31 of the Evaluation report.

³⁴ 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.

³⁵ COM(2005)438 of 21 September 2005, p. 3.

³⁶ See the opinion of 2005, pts. 17-22.

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.³⁷ 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'.³⁸ The Commission concludes that the EU should therefore 'support and regulate data retention as a security measure'.³⁹
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.⁴⁰
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 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*.⁴¹

³⁷ See the speech of 3 December 2010 referred to in footnote 9.

³⁸ All quotes are from p. 23 or 31 of the Evaluation report.

³⁹ See p. 31 of the Evaluation report.

⁴⁰ Czech Republic, Slovenia, UK, Germany, Poland, Finland, Netherlands, Ireland and Hungary.

⁴¹ 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'.

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 of 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.⁴²
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.⁴³ 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.⁴⁴ 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

⁴² See also p. 5 of the Evaluation report.

⁴³ See p. 24 of the Evaluation report.

⁴⁴ See p. 25 of the Evaluation report.

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 (Germany, Rumania and the Czech Republic) 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'.⁴⁵
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 of agricultural funds was annulled.⁴⁶ 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.⁴⁷
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').⁴⁸ 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.

⁴⁵ See p. 31 of the Evaluation report.

⁴⁶ ECJ 9 November 2010, *Volker und Markus Schecke*, C-92/09 and C-93/09.

⁴⁷ ECJ, *Schecke*, para 81.

⁴⁸ '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.

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"*.⁴⁹
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.⁵⁰ 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.

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%.⁵¹ Furthermore, sixteen Member States have chosen a retention period of 1 year or less in their legislation.⁵² This strongly suggests that a

⁴⁹ See p. 5 of the Evaluation report.

⁵⁰ See p. 32 of the Evaluation report.

⁵¹ 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.

⁵² See p. 14 of the Evaluation report.

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".⁵³ 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 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.⁵⁴
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.⁵⁵ 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) 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.⁵⁶ 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.⁵⁷ The law must indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.⁵⁸

⁵³ See p. 30 of the Evaluation report.

⁵⁴ See on this also the EDPS opinion of 2005, pt. 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'.

⁵⁵ See p. 14 of the Evaluation report.

⁵⁶ See ECtHR, *S. and Marper*, referred to in footnote 7, para 151.

⁵⁷ ECJ 20 May 2003, *Österreichischer Rundfunk*, C-465/00, para 77, and ECtHR, *S. and Marper*, referred to in footnote 7, para 95.

⁵⁸ See ECtHR, *Malone*, referred to in footnote 8, paras 66-68.

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".⁵⁹ 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".⁶⁰
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.⁶¹
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".⁶²
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'.⁶³ 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.⁶⁴
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.⁶⁵
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

⁵⁹ COM(2010)573, referred to in footnote 31, p. 5.

⁶⁰ COM(2010)385, referred to in footnote 17, p. 3.

⁶¹ See, for example, ECJ 6 November 2003, *Lindqvist*, para 87.

⁶² See p. 31 of the Evaluation report.

⁶³ ECJ, *Lindqvist*, para 84.

⁶⁴ See also Article 6 of Directive 95/46/EC.

⁶⁵ See p. 8 of the Evaluation report.

and the risk of life and limb".⁶⁶ Member States make use of the 'legal loophole' provided for in Article 15(1) of the ePrivacy Directive.⁶⁷ The Commission considers that this situation may not provide sufficiently for the "foreseeability which is a requirement in any legislative measure which restricts the right to privacy".⁶⁸

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.⁶⁹

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.⁷⁰ 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

⁶⁶ See p. 8 of the Evaluation report.

⁶⁷ As discussed in pt. 24 above.

⁶⁸ See p. 9 and 15 of the Evaluation report.

⁶⁹ See p. 32-33 of the Evaluation report.

⁷⁰ See p. 32-33 of the Evaluation report.

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.⁷¹

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;
- the Data Retention Directive lacks foreseeability.

⁷¹ See Bundesverfassungsgericht, 1 BvR 256/08.

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 in Brussels, 31 May 2011

Peter HUSTINX
European Data Protection Supervisor