I

(Information)

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final)

(2005/C 298/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

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 [1] and on the free movement of such data and 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 (Directive on privacy and electronic communications) [2],

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 [3], and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 23 September 2005 from the Commission;

HAS ADOPTED THE FOLLOWING OPINION:

I **Introduction**

1. The EDPS welcomes the fact that he is consulted on the basis of Article 28(2) of Regulation (EC) No 45/2001. However, in view of the mandatory character of Article 28(2) of Regulation (EC) No 45/2001, the present opinion should be mentioned in the preamble of the directive.

2. The EDPS recognises the importance for law enforcement agencies of the Member States of having all the necessary legal instruments at their disposal, in particular in

[1] OJ L 281, 23.11.1995, p. 31.

[2] OJ L 201, 31.7.2002, p. 37.

[3] OJ L 8, 21.1.2001, p. 1.

the combat of terrorism and other serious crime. An adequate availability of certain traffic and location data of public electronic services can be a crucial instrument for those law enforcement agencies and can contribute to the physical security of persons. In addition it should be noted that this does not automatically imply the necessity of the new instruments as foreseen in the present proposal.

3. It is equally evident that the proposal has a considerable impact on the protection of personal data. If one considers the proposal solely from the perspective of data protection, traffic and location data should not be retained at all for the purpose of law enforcement. It is for reasons of data protection that Directive 2002/58/EC establishes as a principle of law that traffic data must be erased as soon as storage is no longer needed for purposes related to the communication itself (including billing purposes). Exemptions to this principle of law are subject to strict conditions.

4. In this opinion, the EDPS shall highlight the impact of the proposal on the protection of personal data. The EDPS shall furthermore take into account that, not withstanding the importance of the proposal for law enforcement, it may not result in people being deprived of their fundamental right to have their privacy protected.

5. This opinion of the EDPS must be seen in the light of these considerations. The EDPS envisages a balanced approach, in which the necessity and the proportionality of the interference with data protection play a central role.

6. As to the proposal itself, this must be seen as a reaction to the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism ('the draft Framework Decision'), that was rejected by the European Parliament (in the consultation procedure).

7. The EDPS has not been consulted on the draft Framework Decision, nor has he given an opinion on his own initiative. The EDPS does not intend to give as yet an opinion on the draft Framework Decision, but will in the present opinion refer to this draft decision, where he deems this to be useful.

II General observations

The impact of the proposal on the protection of personal data

8. It is essential to the EDPS that the proposal respects the fundamental rights. A legislative measure which would harm the protection guaranteed by Community law and more in particular by the case-law of the Court of Justice and the European Court of Human Rights is not only unacceptable, but also illegal. The circumstances in society may have changed due to terrorist attacks, but this may not have as an effect that high standards of protection in the state of law are compromised. Protection is given by law irrespective of the actual needs of law enforcement. Moreover, the case-law itself allows for exceptions, if necessary in a democratic society.

9. The proposal has a direct impact on the protection given by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the 'ECHR'). According to the case-law of the European Court of Human Rights:

— The storing of information about an individual was considered to be an interference with private life, even though it contained no sensitive data (Amann ([1])).

— The same applies to the practice of 'metering' of telephone calls, which involves the use of a device that registers automatically the numbers dialled on a telephone and the time and the duration of each call (Malone ([2])).

— Justifications for interference should outweigh the detrimental effect that the very existence of the legislative provisions in question could have on the subjects (Dudgeon ([3])).

10. Article 6(2) of the EU-Treaty provides that the Union shall respect fundamental rights, as guaranteed by the ECHR. In the preceding paragraph it has been shown that, under the case-law of the European Court of Human Rights, the obligation to retain data falls within the scope of Article 8 ECHR and that a pressing justification is needed that respects

([1]) Judgment of the ECHR of 16 February 2000, Amann, 2000-II, Appl. 27798/95.

([2]) Judgment of the ECHR of 2 August 1984, Malone, A82, Appl. 8691/79.

([3]) Judgment of the ECHR of 22 October 1981, Dudgeon, A45, Appl. 7525.

the criterion of the Dudgeon-judgement. The necessity and the proportionality of the obligation to retain data — in its full extent — have to be demonstrated.

11. In addition, the proposal has a huge impact on principles of data protection recognised by Community law:

— The data have to be retained over a period far longer than the periods that are usual for retention by providers of publicly available electronic communications services or by a public communications network (both services are hereafter referred to as 'providers').

— Under Directive 2002/58/EC, more in particular its Article 6, data may only be collected and stored for reasons directly related to the communication itself, including billing purposes ([1]). Afterwards, data must be erased (subject to exceptions). Under the present proposal, retention for the purpose of enforcement of criminal law is mandatory. The point of departure is thus contrary.

— Directive 2002/58/EC ensures security and confidentiality. This proposal may not lead to loopholes in that field; strict safeguards are required and the purpose limitation should be clarified.

— The introduction of the obligation to retain data, as foreseen by the proposal, leads to substantial databases and has particular risks for the data subject. One could think of the commercial use of the data, as well as of the use of the data for 'fishing operations' and/or data mining by law enforcement authorities or national security services.

12. Finally, the protection of private life, as well as the protection of personal data have both been recognised in the Charter on Fundamental Rights, as has been mentioned in the Explanatory Memorandum.

13. The impact of the proposal on the protection of personal data needs a thorough analysis. In this analysis, the EDPS will take the foregoing elements into account and he will conclude that more safeguards are needed. A simple reference to the existing legal framework on data protection (in particular, the directives 95/46/EC and 2002/58/EC) is not sufficient.

The necessity of retention of traffic and location data

14. The EDPS recalls the conclusion from 9 November 2004 of the Article 29 Data Protection Working Party on the draft Framework Decision. The Working Party stated that the mandatory retention of traffic data, under the conditions provided for in the draft Framework Decision, is not acceptable. This conclusion was *inter alia* based on the failure to provide any evidence as to the need of the retention for public order purposes, due to the fact that analysis showed that the most significant amount of traffic data demanded by law enforcement was not older than six months.

15. According to the EDPS, the considerations of the Article 29 Data Protection Working Party mentioned above should be the point of departure for the appraisal of the present proposal. However, the result of these considerations can not simply be transposed to the present proposal. One has to take into account that circumstances can change. According to the EDPS, the following developments could be relevant to the appraisal.

16. In the first place, some figures have been produced to demonstrate that in practice traffic data up to one year old are demanded by law enforcement. The Commission as well as the Presidency of the Council attach importance to a study by the police of the United Kingdom ([2]) that shows that although 85 % of the traffic data required by the police was less than six months old, the data between six months and a year were used in complex investigations into more serious crimes. Some examples of cases were presented as well. The retention period in the proposal — one year for telephone data — reflects these practices of law enforcement.

17. The EDPS is not convinced that these figures represent the evidence of the necessity of the retention of traffic data up to one year. The fact that in some cases the availability of traffic and/or location data helped solving a crime does not automatically mean that those data are needed (in general) as a tool for law enforcement. However, the figures can not be ignored. They represent at least a serious attempt to demonstrate the necessity of the retention. Moreover, the figures clearly indicate that a retention period for over one year is not required from the perspective of the current practices of law enforcement.

18. In the second place, the existing possibilities for the providers under Directive 2002/58/EC to retain traffic data for billing purposes are not always used, since in a growing number of cases data retention for billing purposes does not take place at all (prepaid cards for mobile communications,

([1]) See also point 3 of this opinion.

([2]) Liberty and security, striking the right balance. Paper by the UK Presidency of the European Union of 7 September 2005.

flat rate-subscriptions, etc.). In those cases — that in practice have become more frequent — traffic and location data will not be stored at all but erased immediately after the communication. The same goes for unsuccessful calls. This can have an impact on the effectiveness of law enforcement.

19. Moreover, this development in telecommunications services can lead to disturbances in the functioning of the internal market, *inter alia* due to the (imminent) adoption of legislative measures in Member States under Article 15 of Directive 2002/58/EC. For example, the Italian government recently published a decree that obliges providers to store telephone data for four years. This obligation will lead to considerable costs in certain Member States, such as Italy.

20. In the third place, the working methods of law enforcement authorities have developed as well: proactive investigations and the use of technical support have become more important. These developments require that the authorities dispose of adequate and precisely formulated tools to enable them to do their work with due respect to the principles of data protection. One of the tools the authorities in the Member States usually dispose of is data preservation, or, the freezing of communications data on request in a concrete investigation. It has been stated that this tool, that in itself has less impact on those principles than the tool that now is proposed (data retention), might not always be enough, in particular not to track persons involved in terrorism or other serious crime who were previously not suspected of any criminal activity. However, more evidence is needed to determine if this really is the case.

21. In the fourth place, the concerns about terrorist attacks have grown. The EDPS shares the view as expressed in the context of the proposals on data retention, that physical security is, in itself, of overriding importance. Society needs to be protected. For this reason governments are obliged, in case of attacks on society, to demonstrate that they give serious consideration to this need for protection and to investigate if they have to react by introducing new legislative measures. It goes without saying that the EDPS fully endorses the task of governments — on the national as well as on the European level — to protect society and to demonstrate that they do all that is needed to offer protection, including the adoption of new, legitimate and effective measures as a result of their investigations.

22. The EDPS recognises the changes of circumstances, but is as yet not convinced of the necessity of the retention of traffic and location data for law enforcement purposes, as established in the proposal. He emphasises the importance of the principle of law established by Directive 2002/58/EC that traffic data must be erased as soon as storage is no longer needed for purposes that are not related to the communication itself. Furthermore, the figures provided do not prove that the existing legal framework does not offer the instruments that are needed to protect physical security, nor that the Member States fully apply their competences under European law to cooperate as been granted to them within the existing legal framework (but without the results that are needed) .

23. However, if the European Parliament and the Council — after a careful balancing of the interests at stake — draw the conclusion that the necessity of the retention of traffic and location data is sufficiently demonstrated, the EDPS takes the view that the retention can only be justified under Community law in so far as the principle of proportionality is respected and adequate safeguards are provided, in accordance with this opinion.

The proportionality

24. The proportionality of the proposed new legislative measure itself depends on the substance of the provisions it comprises: does it comprise the adequate and proportionate response to the needs of society?

25. The first consideration touches upon the adequacy of the proposal: can one expect that the proposal increases the physical security of the inhabitants of the European Union? One reason to doubt the adequacy, often mentioned in the public debate, is that traffic data and location data are not always linked to a specified individual, so knowledge about a telephone number (or an IP-number) does not necessarily reveal the identity of an individual. Another — and even more serious — reason for doubt is whether or not the existence of gigantic data bases enables law enforcement to easily find what they need in a specific case.

26. The EDPS takes the view that retention of traffic and location data alone is in itself not an adequate or effective response. Additional measures are needed, so as to ensure that the authorities have a targeted and quick access to the data needed in a specific case. The retention of data is only adequate and effective in so far as effective search engines exist.

27. The second consideration touches upon the proportionate nature of the response. To be proportionate, the proposal should:

— limit the retention periods. The periods must reflect the demonstrated needs of law enforcement,

— limit the number of data to be stored. This number must reflect the demonstrated needs of law enforcement and it must be ensured that access to content data is not possible,

— contain adequate safety measures, so as to limit the access and further use, guarantee the security of the data and ensure that the data subjects themselves can exercise their rights.

28. The EDPS emphasises the importance of these strict limitations, with adequate safeguards in view of a limited access. He takes the view that in the perspective of the importance of the three elements mentioned in the foregoing point, the Member States may — as regards these three elements — not take additional national measures that prejudice the proportionality. This need for harmonisation will be elaborated under IV.

Adequate safety measures

29. The effect of the proposal will be that the providers will dispose of databases in which a significant amount of traffic and location data will be stored.

30. In the first place, the proposal will have to make sure that the access to and the further use of these data will be limited, only under specified circumstances and for a limited number of specified purposes.

31. In the second place, the databases will have to be adequately protected (data security). To this effect, it must be ensured that at the end of the retention periods, the data are efficiently erased. There should be no 'dumping of data' or exploitation of data. In short, this requires a high data security and adequate technical and organisational safety-measures.

32. A high data security is even more important since the mere existence of data might lead to demands for access and use, by at least three groups of stakeholders:

— the providers themselves. They might be tempted to use the data for their own commercial goals. Guarantees are necessary, preventing the copying of these files,

— authorities responsible for law enforcement: the proposal offers them a right to access, but only in specific cases and according to national legislation (Article 3(2) of the proposal). There should be no access for data mining purposes or 'fishing operations'. The exchange of data with authorities in other Member States should be clearly regulated,

— intelligence services (with responsibility for national security).

33. As to the access by intelligence services, the EDPS observes that, under Article 33 TEU and Article 64 EC interventions within the third pillar and the first pillar shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security. According to the EDPS, these provisions have as an effect that the European Union lacks the competence to control the access of security or intelligence services to the data retained by the providers. In other words, neither the access of these services to traffic and location data of the providers, nor the further use of the information acquired by these services is affected by the law of the European Union. This is an element that has to be taken into account in the appraisal of the proposal. It is the Member States that should take the necessary measures to regulate the access by intelligence services.

34. In the third place, the effects described in the previous paragraphs have potential implications for the data subject. Additional safeguards are needed so as to make sure that he can simply and quickly exercise his rights as a data subject. The EDPS points out the need of an effective control on the access and further use, preferably by judicial authorities in the Member States. The safeguards should also apply in the case of access and further use of the traffic data by authorities in other Member States.

35. In this context, the EDPS refers to initiatives for a new legal framework on data protection applicable to law enforcement (in the third pillar of the TEU). In his view, such a legal framework requires additional safeguards and could not limit itself to a reaffirmation of the general principles of data protection in the first pillar ([1]).

36. In the fourth place, there is a direct relationship between the adequacy of safety-measures and the costs of these measures. An adequate law on data retention must therefore contain incentives for the providers to invest in the technical infrastructure. Such an incentive could be that the providers are compensated for the additional costs of adequate safety-measures.

37. Summarised, adequate safety-measures should:

— limit the access to and further use of the data,

— provide for adequate technical and organisational safety-measures to protect the databases. This includes the adequate erasure of the data at the end of a retention

([1]) See, in the same sense, the Position Paper on Law Enforcement and Information Exchange in the EU, adopted at the Spring Conference of European Data Protection Authorities, Krakow, 25 to 26 April 2005.

period and which acknowledges the demands for access and use by different groups of stakeholders,

— ensure the exercise of the rights of the data subjects, not just by reaffirming the general principles of data protection,

— contain incentives for the providers to invest in the technical infrastructure.

III The legal basis and the draft framework decision

38. The proposal is based on the EC Treaty, in particular Article 95 thereof, and aims, according to its Article 1, to harmonise the obligations for the providers with respect to the processing and retention of traffic and location data. It states that the data shall only be provided to the competent national authorities in individual cases, related to criminal offences, but it leaves the more precise definition of the purpose as well as the access to and the further use of the data to the discretion of the Member States, subject to the safeguards of the existing Community framework on data protection.

39. In this respect, the proposal has a more limited scope than the draft framework decision that is based on Article 31 (1)(c) TEU and that contains additional provisions on the access to the retained data as well as on requests for access from other Member States. The explanatory memorandum gives a justification of this limitation of the scope of the proposal. It states that access to and exchange of information between relevant law enforcement agencies is a matter which falls outside the scope of the EC Treaty.

40. The EDPS is not convinced by this statement in the explanatory memorandum. An intervention of the Community based on Article 95 EC (internal market) must have the removal of barriers to trade as its main object. According to the case-law of the Court of Justice, such an intervention must be genuinely appropriate for contributing to the removal of such a barrier. However, in its intervention the Community legislator must ensure the respect of fundamental rights (Article 6(2) TEU; see Section II of this opinion). For all that, the establishment on the Community level of rules on the retention of data in the interest of the internal market, may require that also the respect of fundamental rights is dealt with on the level of the European Community. If the Community legislator could not establish rules on the access and the use of data, it could not fulfil its obligation under Article 6 TEU since the latter rules are indispensable in order to ensure that data are retained with due respect to fundamental rights. In other words, according to the EDPS, the rules on the access, the use and the exchange of the data are inseparable from the obligation itself to retain the data.

41. As to the establishment of competent authorities, the EDPS admits that this is the responsibility of the Member States. Likewise is the organisation of the law enforcement and the judicial protection. However, a Community act can impose conditions on the Member States as to the designation of competent authorities, the judicial control or the access to justice by citizens. These provisions ensure that suitable mechanisms exist at a national level to guarantee the full effectiveness of the act, including the full compliance to data protection legislation.

42. The EDPS raises another point, related to the legal basis. It is up to the Community legislature to choose the adequate legal basis and, accordingly, the adequate legislative procedure. This choice goes beyond the mission of the EDPS. However, in the light of the important fundamental issues at stake, the EDPS expresses in the present situation a strong preference for the co-decision procedure. Only this procedure constitutes a transparent process of decision-making with full participation of the three institutions involved and with due respect to the principles on which the Union is founded.

IV The need for harmonisation

43. The proposal for a directive harmonises the types of data to be retained, the periods of time during which the data should be retained, as well as the purposes for which the data may be supplied to the competent authorities. The proposal envisages the full harmonisation of these elements. It is, in this respect, of a fundamentally different nature than the draft Framework Decision, which provides for minimum rules.

44. The EDPS underlines the need for full harmonisation of these elements, in view of the functioning of the internal market, the needs of law enforcement and — last but not least — the ECHR and the principles of data protection.

45. As to the functioning of the internal market, harmonisation of the obligations to retain data justifies the choice of the legal basis of the proposal (Article 95 EC). Allowing essential differences between the laws of the Member States would not take away the existing disturbances in the internal market of electronic communications which are *inter alia* due to the (imminent) adoption of legislative measures in Member States under Article 15 of Directive 2002/58/EC (see point 19 of this opinion).

46. This is even more important since to a notable amount of electronic communications, the jurisdiction of more than one Member State is relevant. Illustrative examples are: cross border phone calls, roaming, border crossing *during* mobile communications, and the use of a provider in another Member State than the country of residence of the individual.

47. Moreover, in this context lack of harmonisation would harm the needs of law enforcement, in so far as the competent authorities have to comply with different legal requirements. This could impede the exchange of information between the authorities of the Member States.

48. Finally, the EDPS emphasises — with a reference to his responsibility under Article 41 of Regulation (EC) No 45/2001 — that full harmonisation of the main elements included in the proposal is indispensable to comply with the ECHR and the principles of data protection. Any legislative measure that obliges to retain traffic and location data has to clearly limit the number of data to be retained, the periods of retention and (the purposes of) the access and further use of the data, in order to be acceptable from the perspective of data protection and to comply with the requirements of necessity and proportionality.

V Comments on the articles of the proposal

Article 3: Obligation to retain data

49. Article 3 is the key provision of the proposal. Article 3(1) introduces the obligation to retain traffic data and location data, whereas Article 3(2) gives effect to the principle of purpose limitation. Article 3(2) lays down three important limitations. The data retained shall only be provided:

— to the competent national authorities,

— in specific cases,

— for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

Article 3(2) refers to the national legislation of the Member States for the specification of further limitations.

50. The EDPS welcomes Article 3(2) as an important provision but deems that the limitations are not precise enough, that the access and further use should explicitly be regulated under the directive and that additional safeguards are needed. As has been said in Section III of this opinion, the EDPS is not convinced that the non-inclusion of (precise) provisions on the access and the further use of the traffic and location data is an inevitable consequence of the legal base of the proposal (Article 95 EC). This leads to the following comments.

51. In the first place: it is not specified that other stakeholders, like the provider himself, do not have access to the data. Under Article 6 of Directive 2002/58/EC, providers may only process traffic data up to the end of the period the data are retained for billing purposes. According to the EDPS there is no justification for access by the providers or by other interested parties otherwise than the access foreseen under Directive 2002/58/EC, and subject to the conditions of that directive.

52. The EDPS recommends adding a provision in the text to ensure that individuals other than the competent authorities do not have access to the data. This provision could be formulated as follows: 'the data may only be accessed and/or processed for the purpose mentioned in Article 3(2)' or 'the providers shall effectively guarantee that access is only granted to the competent authorities'.

53. In the second place: the limitation to specific cases seems to prohibit routine access for 'fishing operations' or for data mining activities. However, the text of the proposal should specify that data can only be provided if this is needed in relation to a specific criminal offence.

54. In the third place: the EDPS welcomes the fact that the purpose of access is limited to serious criminal offences, such as terrorism and organised crime. In other less serious cases, access to traffic and location data will not easily be proportionate. However, the EDPS expresses doubts whether this limitation is precise enough, especially when access will be asked related to serious crime other than terrorism and organised crime. The practice in the Member States will diverge. The EDPS emphasised in section IV of this opinion the need of full harmonisation of the main elements included in the proposal. The EDPS recommends therefore limiting the provision to *certain* serious criminal offences.

55. In the fourth place: Contrary to the draft framework-decision, the proposal does not contain a provision on access. In the view of the EDPS, access to and further use of the data should not be ignored in the directive. They form an inseparable part of the subject-matter (see section III of this opinion).

56. The EDPS recommends the addition to the proposal of one or more articles on the access to the traffic and location data by the competent authorities and on the further use of the data. The objective of these articles should be to ensure that the data are only used for the purposes mentioned in Article 3(2), that the authorities ensure the quality, the confidentiality and the security of the data they have obtained and that the data will be erased when they are no longer

needed for the prevention, investigation, detection and prosecution of the specific criminal offence. Moreover, it should be laid down that access in specific cases should be under judicial control in the Member States.

57. In the fifth place: the proposal does not contain additional safeguards for data protection. The recitals simply refer to safeguards in existing legislation, more in particular Directive 95/46/EC and Directive 2002/58/EC. The EDPS disagrees with this limited approach of data protection in spite of the particular importance of (additional) safeguards (see section II of this opinion).

58. Therefore, the EDPS recommends including a paragraph on data protection. In this paragraph, the preceding recommendations concerning Article 3(2) could be inserted, as well as other provisions on data protection, such as provisions related to the exercise of his rights by the data subject (see section II of this opinion), to data quality and data security, and to traffic and location data of non suspects of criminal offences.

Article 4: Categories of data to be retained

59. In general, the EDPS welcomes the article and the annex, because of:

— the chosen legislative technique with functional descriptions in the body of the directive and technical details in an annex. It is flexible enough to respond adequately to technological developments and it gives legal certainty to the citizen,

— the distinction between data on telecommunications and Internet data, despite the fact that the distinction becomes technologically less important. From the perspective of data protection however, the distinction is important since on the Internet the borderline between content data and traffic data is not clear (see, for example, the recognition in Article 1(2) of the Directive that information consulted on the internet is content data),

— the level of harmonisation: the proposal envisages a high level of harmonisation with an exhaustive list of categories of data to be retained (as opposed to the draft Framework Decision that contains a minimum-list, with a wide margin for the Member States to add data). From the perspective of data protection, full harmonisation is essential (see section IV).

60. The EDPS recommends the following amendments:

— Article 4, second paragraph, should contain more substantial criteria to ensure that content data are not included. The following sentence should be added: 'The Annex may not include data that reveal the content of a communication',

— Article 5 opens up the possibility for the revision of the Annex by a Commission-directive ('comitology'). The EDPS advises that revisions of the Annex with a substantial impact on data protection should preferably be made by way of a directive, in accordance with the co-decision-procedure ([1]).

Article 7: Periods of retention

61. The EDPS welcomes the fact that the retention periods in the proposal are significantly shorter than the periods foreseen in the draft Framework decision:

— Remembering the doubts expressed in this opinion on the evidence of necessity of the retention of traffic data up to one year, the period of one year reflects the practices of law enforcement, *as they have been indicated* by the figures that have been provided by the Commission and the Presidency of the Council.

— These figures show as well that, except for exceptional cases, retention of data for longer periods does not reflect the practices of law enforcement.

— A shorter period of six months for data related to electronic communications taking place using solely or mainly the Internet protocol is important from the perspective of data protection, since the retention of Internet-communications results in vast databases (these data are usually not retained for billing purposes), the borderline with content data is vague and the retention for longer than six months does not reflect the practices of law enforcement.

62. It should be clarified in the text that:

— the retention periods of 6 months, respectively one year are maximum-periods of retention,

([1]) See in the same sense, the Opinion of the EDPS of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (Paragraph 3.12).

— the data are erased at the end of the retention period. The text should also clarify how the data should be erased. According to the EDPS a provider has to erase the data by automated means, at least on a day by day basis.

Article 8: Storage requirements for retained data

63. This article is closely related to Article 3(2) and contains an important provision that can ensure that access in specific cases can be limited to data that are specifically needed. Articles 8 and 3(2) presuppose that the required data are transmitted by the providers to the authorities and that the latter do not have direct access to the databases. The EDPS recommends stating this presumption explicitly in the text.

64. The provision should be specified, by stating that:

— The required data are transmitted by the providers to the authorities (see point 63).

— The providers should install the necessary technical architecture, including search engines, to facilitate the targeted access to the specified data.

— The providers should ensure that only members of their staff with specified technical responsibilities have access to the databases for technical reasons and that those members of staff are aware of the sensitive character of the data and work under strict internal rules of confidentiality.

— The transmission of the data should not only take place without undue delay, but also without revealing other traffic and location data than the data needed for the purposes of the request.

Article 9: Statistics

65. The obligation for providers to supply statistics on a yearly basis helps the Community institutions to monitor the effectiveness of the implementation and application of the present proposal. Adequate information is needed.

66. According to the EDPS, this obligation gives effect to the principle of transparency. The European citizen is entitled to know how effective the data retention is. For this reason, the provider should additionally be obliged to keep logging lists and to perform systematic (self-) auditings, in order to enable the national data protection authorities to control the application of the rules on data protection in practice [1]. The proposal should be amended in that sense.

Article 10: Costs

67. As has been said in section II, there is a direct relationship between the adequacy of safety-measures and the costs of these measures, or in other words between security and costs. The EDPS therefore regards Article 10 — that provides for the reimbursement of demonstrated additional costs — as an important provision that could serve as an incentive for the providers to invest in the technical infrastructure.

68. According to the estimates in the Impact Assessment handed over by the Commission to the EDPS, the costs of data retention are considerable. For a large network and service provider, costs would be more than EUR 150 million, for a 12-month retention period, with annual operating costs of around EUR 50 million [2]. There are no figures, however, on costs of additional security measures, such as expensive search engines (see the comment on Article 6), nor on the (estimated) financial consequences of the full reimbursement of additional costs of the providers.

69. According to the EDPS more precise figures are needed, in order to be able to judge the proposal in its full extent. He suggests clarifying the financial consequences of the proposal in the explanatory memorandum.

70. As to the provision of Article 10 itself, the relationship between the adequacy of safety-measures and the costs should be made clear in the text of the provision. Moreover, the proposal should provide minimum-standards for the safety-measures to be taken by the providers, in order to be entitled to a reimbursement by a Member State. According to the EDPS, the determination of these standards could not be left

[1] See in the same sense, the Opinion of the EDPS of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (Paragraph 3.9).

[2] The Commission refers to figures of ETNO (the EU association of telecommunications operators) and to a report by MEP Alvaro on the draft Framework Decision.

completely to the Member States. This could prejudice the level of harmonisation envisaged by the directive. Furthermore, it should be taken into account that the Member States bear the financial consequences of the reimbursement.

Article 11: Amendment of Directive 2002/58/EC

71. The relation to Article 15(1) of Directive 2002/58/EC should be clarified, since this proposal deprives this provision of much of its content. The references in Article 15(1) of Directive 2002/58/EC to Article 6 and Article 9 (of that same directive) should be deleted, or at least be modified to clarify that the Member States are no longer competent to adopt legislation in relation to criminal offences, additional to the present proposal. Any ambiguity on their remaining competences — for instance as regards the retention of data for the purpose of 'not serious' criminal offences — must be taken away.

Article 12: Evaluation

72. The EDPS welcomes that the proposal contains an article on the evaluation of the Directive, within three years after its entry into force. An evaluation is all the more important in the perspective of the doubts on the necessity of the proposal, and of its proportionality.

73. In this perspective, the EDPS advises to provide for an even stricter obligation, that contains the following elements:

— The evaluation should comprise an assessment of the effectiveness of the implementation of the directive, from the perspective of law enforcement, as well as an assessment of the impact on the fundamental rights of the data subject. The Commission should include any evidence that could affect the evaluation.

— The evaluation should take place on a regular basis (at least every 2 years).

— The Commission should be obliged to submit amendments to the proposal, where appropriate (as in Article 18 of Directive 2002/58/EC).

VI **Conclusions**

Preconditions

74. It is essential to the EDPS that the proposal respects the fundamental rights. A legislative measure which would harm the protection guaranteed by Community law and more in particular by the case-law of the Court of Justice and the European Court of Human Rights is not only unacceptable, but also illegal.

75. The necessity and the proportionality of the obligation to retain data — in its full extent — have to be demonstrated.

76. As to the necessity: the EDPS recognises the changes of circumstances, but is as yet not convinced of the necessity of the retention of traffic and location data for law enforcement purposes, as established in the proposal.

77. Nevertheless, the EDPS presents in this opinion his view on the proportionality of the proposal. This means in the first place, retention of traffic and location data alone is in itself not an adequate or effective response. Additional measures are needed, so as to ensure that the authorities have a targeted and quick access to the data needed in a specific case. In the second place, the proposal should:

— limit the retention periods. The periods must reflect the needs of law enforcement,

— limit the number of data to be stored. This number must reflect the needs of law enforcement and ensure that access to content data is not possible,

— contain adequate safety measures.

General appraisal

78. The EDPS underlines the importance of the fact that the present text of the proposal foresees a full harmonisation of the main elements of the proposal, in particular the types of data to be retained, the periods of time during which the data should be retained, as well as (the purposes of) the access and further use of the data.

79. On some points, further clarifications are needed, for instance to ensure the adequate erasure of the data at the end of a retention period and to effectively prevent access and use by different groups of stakeholders.

80. The EDPS considers the following points essential, for the proposal to be acceptable from the perspective of data protection:

— The addition to the proposal of specific provisions on access to the traffic and location data by the competent authorities and on the further use of the data, as an essential and inseparable part of the subject-matter.

— The addition to the proposal of further additional safeguards for data protection (contrary to a simply reference to safeguards in existing legislation, more in particular Directive 95/46/EC and Directive 2002/58/EC), *inter alia* to ensure the exercise of the rights of the data subjects.

— The addition to the proposal of further incentives to the providers to invest in an adequate technical infrastructure, including financial incentives. This infrastructure can only be adequate in so far as effective search engines exist.

Recommendations for modifications of the proposal

81. As to Article 3(2):

— addition of a provision to ensure that individuals other than the competent authorities do not have access to the data. This provision could be formulated as follows: 'the data may only be accessed and/or processed for the purpose mentioned in Article 3(2)' or 'the providers shall effectively guarantee that access is only granted to the competent authorities':

— specification that data can only be provided if this is needed in relation to a specific criminal offence,

— limitation of the provision to *certain* serious criminal offences,

— addition to the proposal of one or more articles on the access to the traffic and location data by the competent authorities and on the further use of the data, as well as of a provision that access in specific cases should be under judicial control in the Member States,

— inclusion of a paragraph on data protection.

82. As to Articles 4 and 5:

— addition to Article 4, second paragraph, of the following sentence: 'The Annex may not include data that reveal the content of a communication',

— specification that revisions of the Annex with a substantial impact on data protection should preferably be made by way of a directive, in accordance with the co-decision procedure.

83. As to Article 7, a specification in the text that the:

— retention periods of 6 months and one year are maximum-periods of retention,

— data are erased at the end of the retention period. The text should also clarify how the data should be erased, namely by the provider by automated means, at least on a day by day basis.

84. As to Article 8, a specification in the text that:

— the required data are transmitted by the providers to the authorities,

— the providers should install the necessary technical architecture, including search engines, to facilitate the targeted access to the specified data,

— the providers should ensure that only members of their staff with specified technical responsibilities have access to the databases for technical reasons and that those members of staff are aware of the sensitive character of the data and work under strict internal rules of confidentiality,

— the transmission of the data should not only take place without undue delay, but also without revealing other traffic and location data than the data needed for the purposes of the request.

85. As to Article 9:

— addition of a provision that obliges the provider to keep logging lists and to perform systematic (self-) auditings, in order to enable the national data protection authorities to control the application of the rules on data protection in practice.

86. As to Article 10:

— clarification of the relationship between the adequacy of safety-measures and the costs should be made clear in the text of the provision,

— addition of minimum-standards for the safety-measures to be taken by the providers, in order to be entitled to a reimbursement by a Member State,

— clarification of the financial consequences of the proposal in the explanatory memorandum.

87. As to Article 11:

— amendment of Article 15 (1) of Directive 2002/58/EC to delete the references to Article 6 and Article 9 (of that same directive), or at least to modify them in order to clarify that the Member States are no longer competent to adopt legislation in relation to criminal offences, additional to the present proposal.

88. As to Article 12, amendment of the provision of evaluation:

— it should comprise an assessment of the effectiveness of the implementation of the directive,

— it should take place on a regular basis (at least every 2 years),

— the Commission should be obliged to submit amendments to the proposal, where appropriate (like in Article 18 of Directive 2002/58/EC).

Done at Brussels on 26 September 2005.

Peter HUSTINX,

European Data Protection Supervisor