I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive

(2007/C 255/01)

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 and on the free movement of such data [1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2], and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 7 March 2007, the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive [3] was sent by the Commission to the EDPS. In accordance with Article 41 of Regulation (EC) No 45/2001, the EDPS presents this opinion.

2. The Communication reiterates the importance of Directive 95/46/EC [4] as a milestone in the protection of personal data and discusses the Directive and its implementation in three chapters: the past, the present and the future. The central conclusion of the Communication is that the Directive should not be amended. The implementation of the Directive should be further improved by means of other policy instruments, most of them with a non binding nature.

3. This opinion of the EDPS follows the structure of the communication. More importantly, the EDPS shares the central conclusion of the Commission that the Directive should not be amended.

4. However, the EDPS takes this position also for pragmatic reasons. The points of departure for the EDPS are as follows:

— in the short term, energy is best spent on improvements in the implementation of the Directive. As the Communication shows, considerable improvements in the implementation are still possible,

— in the longer term, changes of the Directive seem unavoidable, while keeping its core principles,

— a clear date for a review to prepare proposals leading to such changes should already be set now. Such a date would give a clear incentive to start the thinking about future changes already now.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] Further: the Communication.
[4] Further: 'the Directive'.

5. These points of departure are essential since one has to keep in mind that the Directive operates in a dynamic context. In the first place, the European Union is changing: the free flow of information between the Member States — and between the Member States and third countries — has become more important and will become an even more important reality. In the second place, society is changing. The information society is evolving and has more and more characteristics of a surveillance society ([5]). This implies an increasing need for effective protection of personal data to deal with these new realities in a fully satisfactory way.

II. THE PERSPECTIVES OF THE OPINION

6. In his assessment of the communication, the EDPS will address in particular the following perspectives that are relevant in respect of these changes:

— improvement of the implementation of the Directive itself: how to make data protection more effective? A mix of policy instruments is needed for such an improvement varying from a better communication with society to a stricter enforcement of data protection law,

— the interaction with technology: new technological developments such as developments in data sharing, RFID systems, biometrics and identity managements systems have a clear impact on the requirements for an effective legal framework for data protection. Also, the need for effective protection of the personal data of an individual can impose limitations on the use of these new technologies. Interaction is thus two-sided: the technology influences the legislation and the legislation influences the technology,

— global privacy and jurisdiction issues, dealing with the external borders of the European Union. Whereas the jurisdiction of the Community legislator is limited to the territory of the European Union, the external borders become less relevant for data flows. The economy depends more and more on global networks. Companies based in the European Union increasingly outsource activities, including the processing of personal data to third countries. Moreover, recent cases like SWIFT and PNR confirm that other jurisdictions show interest in 'EU-originating data'. In general, the physical place of a processing operation is less relevant,

— data protection and law enforcement: recent threats to society, whether or not related to terrorism, have led to (demands for) more possibilities for law enforcement authorities to collect, store and exchange personal data. In some cases, private parties are actively involved, as recent cases show. The dividing line with the third pillar of the EU-Treaty (in which area the Directive does not apply) becomes on the one hand more important and on the other hand more fluid. There is even a risk that in certain cases, personal data will not be protected either by first pillar or by third pillar instruments (the 'legal loophole'),

— the consequences, in any event for data protection and law enforcement, of the entry into force of the *Reform Treaty*, now foreseen for 2009.

III. THE PAST AND THE PRESENT

7. The First report on the implementation of the Data Protection Directive of 15 May 2003 contained a Work Programme for better implementation of the data protection Directive, with a list of 10 initiatives to be carried out in 2003 and 2004. The Communication describes how each of these actions has been implemented.

8. On the basis of the analysis of the work conducted under the Work Programme, the Communication draws a positive assessment of the improvements achieved in the implementation of the Directive. The assessment of the Commission, as summarized in the headings of Chapter II ('the present') of the Communication, basically states that: implementation has improved, even though some Member States have not yet implemented properly; some divergences still exist, but they mostly fall within the margin of manoeuvre provided for by the Directive and in any case they do not pose a real problem to the internal market. Legal solutions laid down in the Directive have proved to be substantially appropriate to guarantee the fundamental right to data protection, while coping with evolution in technology and requirements imposed by public interests.

9. The EDPS shares the main lines of this positive assessment. In particular, the EDPS recognizes the considerable work conducted in the field of transborder data flows: findings of adequate protection in respect of third countries, new standard contractual clauses, the adoption of binding corporate rules, the reflection on a more uniform interpretation of Article 26(1) of the Directive and the improvement in notifications under Article 26(2) all go in the direction of facilitating international transfers of personal data. However, the case law of the Court of Justice ([6]) has shown that work still has to be done in this crucial area, in order to cope with developments in both technological and law enforcement fields.

([5]) See point 37 of this Opinion.

([6]) In particular, the judgement of the Court in Lindqvist (see footnote 15) and in the PNR-cases (see footnote 17).

10. The Communication also shows that enforcement and awareness raising are key issues in promoting a better implementation, and that they could be further exploited. Furthermore, exchange of best practices and harmonization in the area of notifications and information provisions represent successful precedents for cutting red tape and reducing costs for firms.

11. In addition, the analysis of the past confirms that improvements cannot be achieved without the involvement of a broad range of stakeholders. The Commission, data protection authorities and the Member States are central actors in most of the actions conducted. However, the role of private parties has an increasing importance, especially when it comes to the promotion of self-regulation and European Codes of Conducts, or to the development of Privacy Enhancing Technologies.

IV. **THE FUTURE**

A. **The conclusion: no change to the Directive now.**

12. There are several reasons for supporting the conclusion of the Commission, that, under the present circumstances and in the short term, no proposal should be envisaged for modification of the Directive.

13. The Commission basically gives two reasons in support of the conclusion. Firstly, the potential of the Directive has not been used to its full extent. Considerable improvements in the implementation of the Directive in the jurisdictions of the Member States are still possible. Secondly, it states that although the Directive leaves a margin of manoeuvre for the Member States, there is no evidence that divergences within this margin pose real problems to the internal market.

14. On the basis of these two reasons, the Commission formulates its conclusion in the following way. It explains what the Directive should do, with emphasis on ensuring trust, and then states that the Directive sets a benchmark, is technologically neutral and continues to provide solid and appropriate responses ([7]).

15. The EDPS welcomes the way in which this conclusion is worded, but is of the opinion that this conclusion could be further reinforced by building it on two additional grounds:

— firstly, the nature of the Directive,

— secondly, the legislative policy of the Union.

The nature of the Directive

16. The fundamental right of natural persons to the protection of their personal data is recognised in Article 8 of the Charter of the Fundamental Rights of the Union and *inter alia* laid down in the Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. In essence, the Directive is a framework containing the main elements of the protection of this fundamental right, by giving substance and amplifying the rights and freedoms included in the Convention ([8]).

17. A fundamental right aims to protect a citizen under all circumstances in a democratic society. The main elements of such a fundamental right should not easily be changed because of developments in society or of the political preferences of ruling governments. For instance, threats to society by terrorist organisations may lead to a different outcome in specific cases because more important interferences might be needed in a person's fundamental right, but may never affect the essential elements of the right itself nor deprive or unduly restrict a private person in the exercise of the right.

18. The second characteristic of the Directive is that it envisages the promotion of the free flow of information in the internal market. Also this second objective can be considered as fundamental, within an ever more developing internal market without internal borders. Harmonisation of essential provisions of national law is one of the main instruments to ensure the establishment and functioning of this internal market. It gives substance to the mutual trust between the Member States in each others national legal systems. Also for these reasons changes should be duly considered. Changes could affect mutual trust.

19. A third characteristic of the Directive is that it must be seen as a general framework upon which specific legal instruments build. These specific instruments include implementing measures of the general framework as well as specific frameworks for specific sectors. The Directive on privacy and electronic communications, 2002/58/EC ([9]), is such a specific framework. Where possible, changing developments in society should lead to changes of implementing measures or specific legal frameworks, not of the general framework on which they build.

The legislative policy of the Union

20. According to the EDPS, the conclusion not to change the Directive now is also the logical consequence of general principles of good administration and legislative policy. Legislative proposals — regardless whether they imply new areas of Community action or amend existing legislative arrangements — should only be submitted if the necessity and proportionality are sufficiently demonstrated. No legislative proposal should be submitted if the same result could be achieved by using other, less far-reaching tools.

([7]) Page 9, first full paragraph of the Communication.

([8]) Recital 11 of the Directive.

([9]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

21. Under the present circumstances, the necessity and proportionality of a modification of the Directive have not been demonstrated. The EDPS recalls that the Directive provides for a general framework for data protection under Community law. It must ensure on the one hand protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data and on the other hand the free flow of personal data within the internal market.

22. Such a general framework should not be amended until it has been fully implemented in the Member States, unless there are clear indications that the objectives of the Directive could not be met under the present framework. In the view of the EDPS, the Commission has — under the present circumstances — adequately substantiated that the potential of the Directive has not been used to its full extent (see Chapter III of this opinion). Equally, there is no evidence that the objectives could not be met under the present framework.

B. **In the longer term changes seem unavoidable**

23. It must be ensured also in future that the principles of data protection will offer effective protection to natural persons, keeping in mind the dynamic context in which the Directive operates (see point 5 of this opinion) and the perspectives of point 6 of this opinion: improvement of the implementation, interaction with technology, global privacy and jurisdiction, data protection and law enforcement, and a Reform Treaty. This need for full application of the data protection principles sets the standards for future changes of the Directive. The EDPS recalls once more that in the longer term changes of the Directive seem unavoidable.

24. As far as the substance of any future measures is concerned, the EDPS provides already at this stage some elements which he considers essential in any future system for data protection within the European Union. These elements include:

— there is no need for new principles, but there is a clear need for other administrative arrangements, which are on the one hand effective and appropriate to a networked society and on the other hand minimise administrative costs,

— the wide scope of data protection law should not change. It should apply to all use of personal data and should not be limited to sensitive data or otherwise be limited to qualified interests or special risks. In other words, the EDPS rejects a 'de minimis' approach as far as the scope of data protection is concerned. This ensures that data subjects will be able to exercise their rights in all situations,

— data protection law should continue to cover a wide variety of situations, but at the same time allow a balanced approach in concrete cases, taking into account other justified (public or private) interests, as well as the need for a minimum of bureaucratic consequences. This system should also allow the possibility for data protection authorities to set priorities and concentrate on areas or issues of special importance or posing specific risks,

— the system should fully apply to the use of personal data for law enforcement purposes, although appropriate additional measures may be necessary to deal with special problems in this area,

— appropriate arrangements should be made for data flow with third countries, as far as feasible based on global standards for data protection.

25. The Communication mentions — in relation to the challenges of new technologies — the ongoing review of Directive 2002/58/EC and the possible need for more specific rules to address data protection issues raised by new technologies such as the Internet and RFID ([10]). The EDPS welcomes this review and further actions, although according to the EDPS they should not solely be related to technological developments, but should take into account the dynamic context in its entirety and in a long term perspective also involve the Directive 95/46/EC. Moreover, more focus is needed in this context. Unfortunately, the Communication has an open end:

— there is no timeline for the realisation of the different activities mentioned in Chapter III of the Communication,

— there is no deadline for a subsequent report on the application of the Directive. Article 33 of the Directive requires that the Commission report 'on regular intervals' but does not specify these intervals either,

— there are no terms of reference: the Communication does not allow for the realisation of the activities foreseen to be measured. It simply refers to the Work Programme presented in 2003,

— there are no indications on the way to proceed in the longer term.

The EDPS suggests that the Commission specifies these elements.

([10]) Page 11 of the Communication.

V. PERSPECTIVES FOR FUTURE CHANGE

A. Full implementation

26. Any future change must be preceded by full implementation of the present provisions of the Directive. Full implementation starts with compliance with the legal requirements of the Directive. The Communication mentions [11] that some Member States have failed to incorporate a number of important provisions of the Directive and points in this respect in particular at provisions for independence of supervisory authorities. It is the task of the Commission to monitor the compliance and where it considers this appropriate use its powers under Article 226 EC.

27. The Communication envisages an interpretative communication on some provisions, in particular those provisions that may lead to formal infringement procedures pursuant to Article 226 EC.

28. In addition, the Directive introduces other mechanisms for the improvement of the implementation. In particular, the tasks of the Article 29 Working Party, listed in Article 30 of the Directive, are designed for this purpose. They are meant to stimulate the implementation in the Member States on a high and harmonised level of data protection beyond what is strictly needed to fulfil the obligations of the Directive. Whilst exercising this role, the Working Party has over the years produced a large number of opinions and other documents.

29. In the view of the EDPS, full implementation of the Directive includes these two elements:

— it should be ensured that the Member States fully comply with their obligations under European law. This means that the provisions of the Directive should be transposed into national law and also in practice the results to be achieved by the Directive should be reached,

— other, non binding tools that could be instrumental to a high and harmonised level of data protection should be fully used.

The EDPS emphasises that both elements should be clearly distinguished, because of the different legal consequences, as well as the related responsibilities. As a rule of thumb: the Commission should take full responsibility for the first element, whereas the Working Party should be the primary actor as far as the second element is concerned.

30. Another, more precise distinction to be made relates to the tools available to achieve better implementation of the Directive. These include:

— implementing measures. Those measures — taken by the Commission through comitology procedure — are foreseen in Chapter IV, on the transfer of personal data to third countries (see Article 25(6) and 26(3)),

— sectoral legislation,

— infringement procedures under 226 EC,

— interpretative communications. Such communications could focus on provisions that may lead to infringement procedures and/or mainly intend to be used as guideline for data protection in practice (see also points 57-62) [12],

— other communications. The Communication of the Commission to the Parliament and the Council on Privacy Enhancing Technologies can be seen as an example,

— promotion of best practices. This tool can be used for a range of subjects, such as administrative simplification, audits, enforcement and sanctions, etc (see also points 63-67).

31. The EDPS suggests to the Commission that it clearly indicates how it will use these different tools when it elaborates its policies on the basis of the present Communication. The Commission should in that context also clearly distinguish its own responsibilities and the responsibilities of the Working Party. Apart from that, it goes without saying that a good cooperation between the Commission and the Working Party is under all circumstances a condition for success.

B. Interaction with technology

32. Point of departure is that the provisions of the Directive are formulated in a technologically neutral way. The Communication links the emphasis on technological neutrality to a number of technological developments, such as the Internet, access services provided in third countries, RFID and the combination of sound and image data with automatic recognition. It distinguishes two types of actions. Firstly, specific guidance as to the application of data protection principles in a changing technological environment with an important role of the Working Party and its Internet Task Force [13]. Secondly, sector specific legislation could be proposed, by the Commission itself.

33. The EDPS welcomes this approach as an important first step. In the longer term however, other and more fundamental steps might be needed. The occasion of this Communication could be used as the start of such a long term approach. The EDPS suggests starting, as a follow up of the present Communication, the discussion on this approach. As possible elements of such an approach, the following points can be mentioned.

[11] Page 6 of the Communication, next to final paragraph.

[12] See, for instance Opinion No 4/2007 on the concept of personal data (WP 137) of the Working Party, adopted at 20 June 2007.

[13] The Internet Task Force is a subgroup of the Article 29 Working Party.

34. In the first place, interaction with technologies works in two ways. On the one hand, new developing technologies may call for modifications of the legal framework for data protection. On the other hand, the need for effective protection of the personal data of individuals may require new limitations or appropriate safeguards on the use of certain technologies, an even further reaching consequence. However, new technologies could also be used effectively and relied upon in a privacy enhancing way.

35. In the second place, some specific limits may be needed if new technologies are used by governmental institutions in the exercise of their public tasks. The discussions on interoperability and access that are taking place in the area of freedom, security and justice relating to the implementation of the Hague Program, are a good example ([14]).

36. In the third place, there is a tendency towards a much wider use of biometric material, such as — but not only — DNA-material. The specific challenges of the use of personal data extracted from this material might have consequences for the laws on data protection.

37. In the fourth place, it has to be acknowledged that society itself is changing and acquires more and more elements of a surveillance society ([15]). A fundamental debate is needed on this development. In such a debate central questions would be whether this development is unavoidable, whether it is the task of the European legislator to interfere in this development and to impose limits on this development, whether and how the European legislator could take effective measures, etc.

C. **Global privacy and jurisdiction**

38. The perspective of global privacy and jurisdiction plays a limited role within the Communication. The only intention in this context is that the Commission will continue to monitor and contribute to international forums, to ensure coherence of Member States' commitments with their obligations under the Directive. Apart from that, the Communication enumerates a number of activities executed for the simplification of the requirements for international transfers (see Chapter III of this opinion).

39. The EDPS regrets that this perspective has not been given a more prominent role in the Communication.

40. Presently, Chapter IV of the Directive (Articles 25 and 26) introduces a special regime for transfer of data to third countries, on top of the general rules on data protection. This special regime has been elaborated over the years, with the intention of striking a fair balance between the protection of the individuals whose data are to be transferred to third countries with, inter alia, the imperatives of international trade and the reality of global telecommunications networks. The Commission and the Working Party ([16]), but also for instance the International Chamber of Commerce, have invested much effort in making this system work, through adequacy findings, standard contractual clauses, binding corporate rules, etc.

41. For the applicability of the system to Internet, the judgement of the Court of Justice in *Lindqvist* ([17]) has been of specific importance. The Court points at the ubiquitous nature of information on Internet and decides that the loading of data onto an internet page as such, even if those data are thereby made accessible to persons in third countries with the technical means to access them, does not qualify as a transfer to a third country.

42. This system, a logical and necessary consequence of the territorial limitations of the European Union, will not provide full protection to the European data subject in a networked society where physical borders lose importance (see, examples mentioned in point 6 of this opinion): the information on Internet has an ubiquitous nature, but the jurisdiction of the European legislator is not ubiquitous.

43. The challenge will be to find practical solutions that reconcile the need for protection of the European data subjects with the territorial limitations of the European Union and its Member States. The EDPS — in his comments on the Commission communication on a Strategy on the External Dimension of the Area of Freedom, Security and Justice — has already encouraged the Commission to take a proactive role in promoting the protection of personal data at international level, by supporting bilateral and multilateral approaches with third countries and cooperation with other international organisations ([18]).

([14]) See, for instance, Comments on the Communication of the Commission on interoperability of European databases, 10 March 2006, published on the website of the EDPS.

([15]) See: 'Report on the Surveillance Society', prepared by the Surveillance Studies Network for the UK Information Commissioner, and presented at the 28th International Conference of Data Protection and Privacy Commissioners in London on 2-3 November 2006 (see: www.privacyconference2006.co.uk (section Documents)).

([16]) See, for instance, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, adopted on 25 November 2005 (WP 114); Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From 'Binding Corporate Rules', adopted on 14 April 2005 (WP 107), and Opinion No 8/2003 on the draft standard contractual clauses submitted by a group of business associations ('the alternative model contract'), adopted on 17 December 2003 (WP 84).

([17]) Judgment of the Court of 6 November 2003, Case C-101/01, ECR [2003], p. I-12971, points 56-71.

([18]) See Letter to the Director General of the European Commission's Justice, Freedom and Security department on the Communication on 'A Strategy on the External Dimension of the Area of Freedom, Security and Justice', 28 November 2005, available at EDPS website.

44. Such practical solutions include:

— further development of a Global Framework for data protection. More generally accepted standards such as the OECD-guidelines for data protection (1980) and UN-Guidelines could be used as basis,

— further development of the special regime for transfer of data to third countries, as included in Chapter IV of the Directive (Articles 25 and 26),

— international agreements on jurisdiction, or similar agreements with third countries,

— investing in mechanisms for global compliance, such as the use of binding corporate rules by multinational companies, regardless of where personal data are processed by them.

45. None of these solutions are new. However, a vision is needed on how to effectively use these methods in the most effective way and how to make sure that data protection standards — that in the European Union are qualified as fundamental rights — will also be effective in a global networked society. The EDPS invites the Commission to start developing such a vision, together with most relevant stakeholders.

D. **Law enforcement**

46. The Communication pays extensive attention to requirements imposed by public interests, especially for security. It explains Article 3(2) of the Directive and the interpretation given by the Court of Justice to this provision in the PNR-Judgment ([19]), as well as Article 13 of the Directive, *inter alia* related to the case law of the European Court of Human Rights. The Communication furthermore stresses that when the Commission strikes the balance between measures to ensure security and non negotiable fundamental rights, it makes sure that personal data are protected as guaranteed by Article 8 ECHR. This point of departure also applies to the transatlantic dialogue with the United States of America.

47. According to the EDPS, it is important that the Commission reiterates in such a clear manner the obligations of the Union under Article 6 of the EU Treaty to respect fundamental rights, as guaranteed by the ECHR. This statement is even more important now the European Council has decided that, under the *Reform Treaty*, the Charter of the fundamental rights of the European Union should have legally binding value. Article 8 of the Charter specifies everyone's right to protection of personal data concerning him or her.

48. It is common knowledge that the demands of law enforcement to increasingly use personal data for the combat of crime — not to mention the fight against terrorism — run the risk of lowering the level of protection of the citizen, even below a level that is guaranteed by Article 8 ECHR and/or the Council of Europe Convention No 108 ([20]). These concerns were a main element of the third opinion of the EDPS on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, issued on 27 April 2007.

49. It is in this context essential that the standard of protection provided for by the Directive be taken as a basis for the protection of the citizen, also in relation to demands of law enforcement. The ECHR and Convention 108 provide for a minimal level of protection, but do not provide for the necessary precision. Over and above that, additional measures were needed to provide for appropriate protection for the citizen. This need was one of the driving factors of the adoption in 1995 of the Directive ([21]).

50. It is equally essential that this standard of protection is effectively guaranteed in all situations where personal data are processed for law enforcement purposes. Although this communication does not deal with data processing in the third pillar, it rightly addresses the situation where data collected (and processed) for commercial purposes are used for law enforcement purposes. A situation, which is becoming more usual since police work relies more and more on the availability of information in possession of third parties. Directive 2006/24/EC ([22]) can be seen as the best illustration of this trend: this directive obliges providers of electronic communications to (longer) store data they have collected (and stored) for commercial purposes, for purposes of law enforcement. According to the EDPS, it should be fully ensured that personal data collected and processed within the scope of application of the Directive are properly protected when used for public interest purposes, and in particular for security or fight against terrorism. In some cases however, the latter purposes may fall beyond the scope of the Directive.

([19]) Judgment of the Court of 30 May 2006, European Parliament v Council (C-317/04) and Commission (C-318/04), Joined Cases C-317/04 and C-318/04, ECR [2006], p. I-4721.

([20]) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.

([21]) The lack of precision of Convention No 108 was mentioned by the EDPS in a number of opinions, in relation to the need for a Council Framework Decision.

([22]) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

51. These observations lead to the following suggestions to the Commission:

— further reflection is needed on the implications to data protection of the involvement of private companies in law enforcement activities, with a view to ensuring that the principles of Directive 95/46/EC are fully applicable to these situations and that no lacunae affect citizens' fundamental right to data protection. In particular, it should be ensured that personal data collected within the scope of the Directive are properly and consistently protected also when further processed for public interests, be it within or beyond the scope of the Directive,

— this reflection should include in any event the shortcomings of the present legal framework where the borderline between the first and the third pillar is unclear and where there might even be situations in which there is no appropriate basis for a legal instrument for data protection at all ([23]),

— Article 13 of the Directive, allowing exemptions and restrictions to data protection principles when this is necessary *inter alia* for public interests, should be construed in a way to preserve its *effet utile* as crucial interface and guarantee for personal data collected within the scope of the Directive, in line with the judgement of the Court of Justice in *Österreichischer Rundfunk* ([24]) and the case law of the ECHR,

— the possibility of proposing legislation aiming at harmonizing the conditions and the safeguards for using the exemptions of Article 13 should be considered.

E. **The possible situation under the Reform Treaty**

52. In the Communication, the Commission touches upon the — enormous — impact of the Constitutional Treaty on the field of data protection. Indeed, the Treaty — which is now the Reform Treaty — will be of crucial importance in this field. The Treaty will be the end of the pillar structure, the provision on data protection (currently Article 286 EC) will be clarified and the Charter on the Fundamental Rights of the Union, which includes in its Article 8 a provision on data protection, will become a binding instrument.

53. The mandate for the Intergovernmental Conference (IGC) pays specific attention to data protection. Point 19(f) basically states three things. Firstly, the general rules on data protection will be without prejudice to specific rules adopted in the CFSP Title (the current second pillar); secondly, a declaration will be adopted on data protection in the areas of police and judicial cooperation in criminal matters (the current third pillar) and thirdly, specific entries in the relevant Protocols will be adopted on the position of individual Member States (this element is mainly related to the specific position of the United Kingdom as regards police and judicial cooperation in criminal matters).

54. It is the second element (the declaration) that will need clarification in the IGC. The consequences of the end of the pillar structure and the possible applicability of the Directive on police and judicial cooperation in criminal matters have to be duly considered, so as to ensure the widest possible application of the data protection principles contained in the Directive. This is not the place for further details on this issue. The EDPS has presented suggestions for the declaration in a letter to the Presidency of the IGC ([25]).

VI. **INSTRUMENTS FOR BETTER IMPLEMENTATION**

A. **General**

55. The Communication refers to a series of tools and actions that can be used for a better implementation of the Directive in the future. The EDPS wishes to comment on them, while also exploring other additional instruments not mentioned in the Communication.

B. **Sectoral legislation**

56. In certain cases, specific legislative action at EU level may be necessary. In particular, sectoral legislation may prove to be necessary in order to adapt the Directive's principles to issues raised by some technologies, as it was in the case of the directives on privacy in the telecommunication sector. The use of specific legislation should be carefully considered in domains such as the use of RFID technologies.

C. **Infringement procedures**

57. The most powerful instrument mentioned in the Communication is the infringement procedure. The Communication identifies one specific area of concern, namely the independence of data protection authorities and their powers, and only mentions in general terms other areas. The EDPS shares the view that infringement procedures are an essential and unavoidable instrument, if Member States do not provide for a full implementation of the Directive, especially taking into account that almost nine years have elapsed since the deadline for implementation of the Directive and that the structured dialogue laid down in the Work Programme has already taken place. However, as of today, no case of infringement of Directive 95/46 has yet been brought before the Court of Justice.

([23]) The issue of a 'legal loophole', as expressed by the EDPS on several occasions, mainly in relation to the PNR-Judgement (see, f.i. annual report 2006, p. 47).

([24]) Judgment of the Court of 20 May 2003, Joined Cases C-465/00, C-138/01 and C-139/01, ECR [2003] p. I-4989.

([25]) See EDPS letter of 23 July 2007 to the IGC presidency on data protection under the Reform treaty, available at EDPS website.

58. A comparative analysis of all cases where wrong or incomplete transposition is suspected ([26]), as well as an interpretative communication may certainly improve the coherence of the Commission's role as guardian of the Treaties. However, the preparation of these instruments, that might require a certain amount of time and effort, should not delay infringement procedures in those areas where an incorrect transposition or practice has already been clearly identified by the Commission.

59. Therefore, the EDPS encourages the Commission to pursue a better implementation of the Directive through infringement procedures, where necessary. In this context, the EDPS will make use of his powers of intervention before the Court of Justice in order to intervene, where appropriate, in infringement procedures relating to the implementation of Directive 95/46 or to other legal instruments in the area of the protection of personal data.

D. **Interpretative communication**

60. The Communication also refers to an interpretative communication on some provisions in which the Commission will clarify its understanding of provisions of the Directive, whose implementation is found to be problematic and may thus lead to infringement procedures. The EDPS welcomes that in this context the Commission will take into account the work on interpretation conducted by the Working Party. Indeed, it is essential that the position of the Working Party is duly taken into account when drafting the upcoming interpretative communication and that the Working Party is properly consulted, with a view to bringing in its experience in the application of the Directive at national level.

61. Furthermore, the EDPS confirms his availability to advise the Commission in all matters relating to the protection of personal data. This also applies to those instruments, such as Commission communications, that are not binding but are still aimed at defining the Commission policy in the area of the protection of personal data. In the case of communications, for this advisory role to be effective, the consultation of the EDPS should take place before the interpretative communication is adopted ([27]). The advisory role of both the WP 29 and the EDPS will provide added value to this communication, while preserving the independence of the Commission in deciding autonomously about formally opening infringement procedures relating to the implementation of the Directive.

62. The EDPS welcomes that the communication will deal only with a limited number of Articles, thus allowing focusing on more sensitive issues. In this perspective, the EDPS draws the Commission's attention to the following issues, which deserve special attention in the interpretative communication:

— the concept of personal data ([28]),

— the definition of the role of data controller or data processor,

— the determination of applicable law,

— purpose limitation principle and incompatible use,

— legal grounds for processing, especially with regard to unambiguous consent and balance of interests.

E. **Other, non binding instruments**

63. Other, non binding instruments should proactively develop compliance with data protection principles, particularly in new technological environments. These measures should build on the concept of 'privacy by design', ensuring that the architecture of new technologies is developed and constructed by taking properly into account the principles of data protection. The promotion of privacy-compliant technological products should be a crucial element in a context in which ubiquitous computing is fast developing.

64. Closely linked is the necessity to extend the gamut of stakeholders in the enforcement of data protection law. On the one hand, the EDPS strongly supports the fundamental role of data protection authorities in enforcing the principles of the Directive, making full use of their powers as well as of the scope for coordination within the Article 29 Working Party. A more effective enforcement of the Directive is also one of the objectives of the 'London initiative'.

65. On the other hand, the EDPS stresses the desirability of promoting private enforcement of data protection principles through self-regulation and competition. Industry should be encouraged to implement data protection principles and compete in developing privacy-compliant products and services as a way of expanding its position on the market by better addressing the expectations of privacy-aware consumers. In this context a good example can be found in Privacy seals, that could be attached to products and services that have undergone a certification procedure ([29]).

([26]) See the Communication, p. 6.

([27]) See EDPS Policy Paper 'The EDPS as an advisor to the Community Institutions on proposals for legislation and related documents', available at EDPS website (point 5.2 of the paper).

([28]) This subject was also dealt with in Opinion No 4/2007 of the Working Party, cited in footnote 9.

([29]) It is worth mentioning the EuroPriSe project, promoted by the Schleswig Holstein Data Protection Authority within the Framework of the Eten project of the European Commission.

66. The EDPS would also like to draw the Commission's attention to other tools that, though not mentioned by the Communication, could prove to be useful for a better implementation of the Directive. Examples of such tools that would help data protection authorities in better enforcing data protection law are:

— benchmarking,

— promoting and sharing best practices,

— third-party privacy audits.

F. **Other instruments, for the longer term**

67. As a last point, the EDPS refers to other instruments that are not mentioned in the Communication, but could be either considered for a future change of the Directive or included in other horizontal legislation, in particular:

— class actions, empowering groups of citizens to jointly use litigation in matters concerning protection of personal data, might constitute a very powerful tool to facilitate the enforcement of the Directive,

— actions, initiated by legal persons whose activities are designed to protect the interests of certain categories of persons, such as consumer associations and trade unions, might have a similar effect,

— obligations for data controllers to notify security breaches to data subjects would not only be a valuable safeguard, but also a way of raising awareness among citizens,

— provisions facilitating the use of privacy seals or third-party privacy audits (see points 65 and 66) in a transnational setting.

G. **Better defining the responsibilities of the institutional actors, in particular the Working Party**

68. Different institutional actors have responsibilities relating to the implementation of the Directive. The supervisory authorities in the Member States are under Article 28 of the Directive responsible for the monitoring of the application of the national provisions transposing the Directive in the Member States. Article 29 introduces the Working Party of supervisory authorities whilst Article 30 enumerates its tasks. Under Article 31 a committee of representatives from the Governments of the Member States assists the Commission in relation to implementing measures on Community level (a comitology-committee).

69. The need for better defining the responsibilities of the different actors exists in particular in relation to (the activities of) the Working Party. Article 30(1) lists four tasks of the Working Party which can be summarized as examining the application of the Directive on the national level with a view to uniformity and giving opinions on developments on Community level: the level of protection, legislative proposals and codes of conduct. This list shows the wide responsibility of the Working Party in the area of data protection, which is furthermore illustrated by the documents produced by the Working Party over the years.

70. According to the Communication, the Working Party 'is a key element in ensuring better and more coherent implementation.' The EDPS fully subscribes this statement, but also deems it necessary to clarify some specific elements of the responsibilities.

71. Firstly, the Communication urges for improvement of the contribution of the Working Party, since the national authorities should strive to adapt their national practice to the common line ([30]). The EDPS welcomes the intention of this statement, but warns for a confusion of responsibilities. It is the task of the Commission under Article 211 EC to monitor the compliance in the Member States, including the compliance by the supervisory authorities. The Working Party as an independent advisor can not be held responsible for the application by the national authorities of its opinions.

72. Secondly, the Commission must be aware of its different roles in the Working Party, since it is not only a Member of the Working Party, but also provides its secretariat. In the exercise of the second role as secretariat, it must support the Working Party in a way that it can do its work in an independent manner. This basically means two things: the Commission must provide the necessary resources and the secretariat must work under the instructions of the Working Party and its Chairman as to the content and the scope of the Working Party's activities, as well as the nature of its output. More in general, the activities of the Commission in the fulfilment of its other duties under EC law should not impinge on its availability as a secretariat.

73. Thirdly, although the choice of priorities of the Working Party is the discretion of the Working Party itself, the Commission could indicate what it expects from the Working Party and how it considers that the available resources can at best be used.

74. Fourthly, the EDPS regrets that the Communication does not give clear indications on the division of roles between the Commission and the Working Party. He invites the Commission to present a paper to the Working Party in which such indications are given. The EDPS has the following suggestions for issues to be included in this paper:

— the Commission could ask the Working Party to work on a number of concrete and specified issues. The requests of the Commission should be based on a clear strategy of the tasks and priorities of the Working Party,

([30]) See page 11 of the Communication.

— the Working Party sets its own priorities in a Work Program with clear priorities,

— possibly, the Commission and the Working Party could lay down their arrangements in a Memorandum of Understanding,

— it is essential that the Working Party is fully involved in the interpretation of the Directive and feeds the discussions leading to possible changes of the Directive.

VII. **CONCLUSIONS**

75. The EDPS shares the central conclusion of the Commission that the Directive should not be amended in the short term. This conclusion could be reinforced by building it also on the nature of the Directive and on the legislative policy of the Union.

76. The points of departure for the EDPS are as follows:

— in the short term, energy is best spent on improvements in the implementation of the Directive,

— in the longer term, changes of the Directive seem unavoidable,

— a clear date for a review to prepare proposals leading to such changes should already be set now. Such a date would give a clear incentive to start the thinking about future changes already now.

77. The main elements for future change include:

— no need for new principles, but a clear need for other administrative arrangements,

— the wide scope of data protection law applicable to all use of personal data should not change,

— data protection law should allow a balanced approach in concrete cases and should also allow data protection authorities to set priorities,

— the system should fully apply to the use of personal data for law enforcement purposes, although appropriate additional measures may be necessary to deal with special problems in this area.

78. The EDPS suggests that the Commission specifies: a timeline for the activities of Chapter III of the Communication; a deadline for a subsequent report on the application of the Directive; terms of reference to measure the realisation of the activities foreseen; indications on the way to proceed in the longer term.

79. The EDPS welcomes the approach on technology as an important first step and suggests starting the discussion on a long term approach, including *inter alia* a fundamental debate on the development of a surveillance society. He also welcomes the ongoing review of Directive 2002/58/EC and the possible need for more specific rules to address data protection issues raised by new technologies such as the Internet and RFID. These actions should take into account the dynamic context in its entirety and in a long term perspective also involve the Directive 95/46/EC.

80. The EDPS regrets that the perspective of global privacy and jurisdiction plays a limited role in the Communication and asks for practical solutions that reconcile the need for protection of the European data subjects with the territorial limitations of the European Union and its Member States, such as: the further development of a Global Framework for data protection; the further development of the special regime for transfer of data to third countries; international agreements on jurisdiction or similar agreements with third countries; investing in mechanisms for global compliance, such as the use of binding corporate rules by multinational companies.

The EDPS invites the Commission to start developing a vision on this perspective, together with most relevant stakeholders.

81. On law enforcement, the EDPS has the following suggestions to the Commission:

— further reflection on the implications of the involvement of private companies in law enforcement activities,

— preserve the *effet utile* of Article 13 of the Directive, possibly by proposing legislation aiming at harmonizing the conditions and the safeguards for using the exemptions of Article 13.

82. Full implementation of the Directive means (1) that it be ensured that the Member States fully comply with their obligations under European law and (2) that other, non binding tools, that could be instrumental to a high and harmonised level of data protection be fully used. The EDPS asks from the Commission to clearly indicate how it will use the different instruments and how it distinguishes its own responsibilities from those of the Working Party.

83. As to those instruments:

— in certain cases, specific legislative action at EU level may be necessary,

— the Commission is encouraged to pursue a better implementation of the Directive through infringement procedures,

— the Commission is invited to use the instrument of an interpretative communication — whilst respecting the advisory role of both the Working Party and the EDPS — for the following issues: the concept of personal data; the definition of the role of data controller or data processor; the determination of applicable law; the purpose limitation principle and incompatible use; legal grounds for processing, especially with regard to unambiguous consent and balance of interests,

— non binding instruments include instruments building on the concept of 'privacy by design',

— for longer term also: class actions; actions initiated by legal persons whose activities are designed to protect the interests of certain categories of persons; obligations for data controllers to notify security breaches to data subjects; provisions facilitating the use of privacy seals or third-party privacy audits in a trans-national setting.

84. The EDPS invites the Commission to present a paper to the Working Party giving clear indications on the division of roles between the Commission and the Working Party, including the following issues:

— requests of the Commission to work on a number of concrete and specified issues, based on a clear strategy of the tasks and priorities of the Working Party,

— the possibility to lay down arrangements in an MoU,

— full involvement of the Working Party in the interpretation of the Directive and the discussions leading to possible changes of the Directive.

85. The consequences of the Reform Treaty have to be duly considered, so as to ensure the widest possible application of the data protection principles contained in the Directive. The EDPS has presented suggestions in a letter to the Presidency of the IGC.

Done at Brussels, 25 July 2007.

Peter HUSTINX

European Data Protection Supervisor