Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen

(2009/C 276/02)

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,

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, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 10 June 2009, the Commission adopted its Communication to the European Parliament and the Council on an area of freedom, security and justice serving the citizen ([1]). In accordance with Article 41 of Regulation (EC) No 45/2001, the EDPS presents this opinion.

2. Prior to the adoption of the Communication, the Commission informally consulted the EDPS on it, by letter of 19 May 2009. The EDPS responded to this consultation on 20 May 2009 by sending informal comments which were intended to further improve the text of the Communication. Furthermore, the EDPS has actively contributed to the letter of 14 January 2009 of the Working Party on Police and Justice on the multi-annual programme in the Area of freedom, security and justice ([2]).

3. The Communication (paragraph 1) emphasises that the Union 'needs a new multi-annual programme that builds on the progress made so far and learns the lessons of the current weaknesses in order to make an ambitious push forward. The new programme should define the priorities for the next five years'. This multi-annual programme (already known as the Stockholm programme) will be the follow up of the Tampere and Hague programmes which gave a strong political impetus to the Area of freedom, security and justice.

4. The Communication is meant to be the basis of this new multi-annual programme. The EDPS notes in this context that, even if multi-annual programmes are not as such binding instruments, they have a considerable impact on the policy that the institutions will develop in the area concerned, as many of the concrete legislative and non-legislative actions will stem from the programme.

5. The Communication itself must be seen in this perspective. It is the next step in a debate which more or less started with two reports presented in June 2008 of the so-called 'Future Groups' set up by the presidency of the Council to provide ideas: 'Freedom, Security, Privacy — European Home Affairs in an open world' ([3]) and 'Proposed Solutions for the Future EU Justice Programme' ([4]).

II. MAIN CONTENT OF THE OPINION

6. The present opinion not only provides a reaction to the Communication, but is also a contribution of the EDPS to the more general debate on the future of the Area of freedom, security and justice which must result in a new strategic work programme (the Stockholm programme) as announced by the Swedish presidency of the EU ([5]). This opinion will also deal with some consequences of the possible entry into force of the Lisbon Treaty.

7. After a specification of the main perspectives of the Opinion in Part III, a general assessment of the Communication will be given in Part IV.

8. Part V deals with the question how to respond to the need for continued respect for the protection of privacy and personal data in a context of increasing exchanges of personal data. The focus will be on paragraph 2.3 of the Communication on protection of personal data and privacy, and more in general the needs for further legislative and non-legislative actions to improve the framework for data protection.

([1]) COM(2009) 262 final ('the Communication').

([2]) Not published. The Working Party on Police and Justice (WPPJ) was established by the European Conference of Data Protection Commissioners to prepare its positions in the area of law enforcement, and to act on its behalf in urgent matters.

([3]) Council Document No 11657/08. Hereinafter 'the Home Affairs Report'.

([4]) Council Document No 11549/08 ('the Justice Report').

([5]) The Government's EU work programme, http://www.regeringen.se

9. Part VI discusses the needs and possibilities for the storage, access and exchange of information as instruments for law enforcement, or in the words of the Communication, for 'a Europe that protects'. Paragraph 4 of the Communication contains a number of objectives on the flow of information and technological tools, in particular in paragraphs 4.1.2 (Controlling the flow of information), 4.1.3 (Mobilising the necessary technological tools) and 4.2.3.2 (Information Systems). The development of a European information model (in paragraph 4.1.2) can be seen as the most challenging proposal in this context. The EDPS opinion analyses this proposal in depth.

10. Part VII briefly touches upon a specific topic within the Areas of freedom, security and justice with relevance for data protection, namely access to justice and e-Justice.

III. **PERSPECTIVES OF THE OPINION**

11. This opinion will take the need for protection of fundamental rights as main angle for the analysis of the Communication and more in general the future of the Area of freedom, security and justice, as shaped by a new multi-annual programme. It will furthermore build on the contributions of the EDPS to the development of the EU policy in this area, mainly in his consultative role. Until now, the EDPS has adopted more than 30 opinions and comments about initiatives stemming from the Hague programme which all can be found on the website of the EDPS.

12. In his assessment of the Communication, the EDPS will take into account in particular the following four perspectives that are relevant for the future of the Area of freedom, security and justice. All these perspectives have a key role in the Communication as well.

13. The first perspective is the exponential growth of digital information on citizens as a result of evolving information and communication technologies ([6]). The society is moving towards what is often called a 'surveillance society' in which every transaction and almost every move of the citizens is likely to create a digital record. The so-called Internet of things and 'ambient intelligence' are already developing fast through the use of RFID tags. Digitalised characteristics of the human body (biometrics) are increasingly used. This leads to an increasingly connected world in which public security organisations may have access to vast amounts of potentially useful information, which can directly affect the life of the persons concerned.

14. The second perspective is internationalisation. On the one hand, in the digital age data exchange is not bound by the external borders of the European Union, while on the other hand there is an increasing need of international cooperation in the whole range of EU activities in the Area of freedom, security and justice: fight against terrorism, police and judicial cooperation, civil justice and border control are only some examples.

15. The third perspective is the use of data for law enforcement purposes: 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 many cases, private parties are actively involved, as, inter alia, shown by the Data Retention Directive ([7]) and the various instruments relating to PNR ([8]).

16. The fourth perspective is free movement. The gradual development of an area of freedom, security and justice requires that the internal borders and possible barriers for free movement within the area are further removed. New instruments in this area should in any event not reinstall barriers. Free movement comprises in the present context, on the one hand, the free movement of persons, and on the other hand, the free movement of (personal) data.

17. These four perspectives demonstrate that the context in which information is used is changing rapidly. In such a context, there can be no doubt about the importance of a strong mechanism for the protection of fundamental rights of the citizen, and in particular privacy and data protection. It is for these reasons that the EDPS chooses the need for protection as main angle for his analysis, as mentioned in point 11.

([6]) The Home Affairs Report speaks in this context even of a 'digital tsunami'.

([7]) 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.

([8]) See e.g. Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), OJ L 204, 4.8.2007, p. 18 and Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final.

IV. GENERAL ASSESSMENT

18. The Communication and the Stockholm programme are set to specify the intentions in the EU for the coming five years, with effects possibly on an even longer term. The EDPS notes that the Communication is written in a so-called Lisbon neutral-manner. The EDPS understands fully why the Commission has taken this approach, but also regrets that the Communication could not fully take advantage of the additional possibilities offered by the Lisbon Treaty. The perspective of the Lisbon Treaty will be given more emphasis in this opinion.

19. The Communication builds on the results of the actions of the EU in the Area of freedom, security and justice in recent years. Those results can be characterised as event driven, with an emphasis on measures extending the powers of law enforcement authorities and intrusive for the citizen. This is certainly the case in the domains where personal data are intensively used and exchanged and that are therefore crucial for data protection. The results are event driven since external events, like 9/11 and the bombings in Madrid and London, gave a strong impetus to legislative activities. For instance, the transfer of passenger data to the United States can be seen as the consequence of 9/11 ([9]), whereas the London bombings led to the Data Retention Directive 2006/24/EC ([10]). The emphasis was on more intrusive measures, since the EU legislator focused on measures that facilitate data use and exchange whereas measures aiming to guarantee the protection of personal data were discussed with less urgency. The main protective measure that was adopted is Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters ([11]), after discussions of three years in Council. The result was a Council framework decision that is not fully satisfactory (see points 29-30).

20. The experience in recent years demonstrates that there is a need for reflection on the consequences for law enforcement authorities and for European citizens before new instruments are adopted. This reflection should duly take into account the costs for privacy and the effectiveness for law enforcement, in the first place when new instruments are proposed and discussed, but also after those instruments are implemented, by means of periodic reviews. Such reflection is also essential before a new multi-annual programme is to set out main initiatives for the near future.

21. The EDPS is glad that the Communication recognises the protection of fundamental rights, and in particular the protection of personal data, as one of the key issues of the future of the Area of freedom, security and justice. Paragraph 2 of the Communication qualifies the EU as a unique area for the protection of fundamental rights based on common values. It is also good that the accession to the European Convention on Human Rights is mentioned as priority issue — even the first priority issue in the Communication. Accession is an important step forward in ensuring a harmonious and coherent system for the protection of fundamental rights. Last but not least, data protection has been given a prominent place in the Communication.

22. This focus of the Communication shows a strong intention to ensure the protection of the rights of the citizen and — by doing so — take a more balanced approach. Governments need appropriate instruments to guarantee the security of the citizen, but within our European society they have to fully respect the citizen's fundamental rights. Serving the citizen ([12]) requires a European Union that guards this balance.

23. In the view of the EDPS, the Communication takes the need for this balance very well into account, including the need for protection of personal data. It recognises the need for a change of emphasis. This is important since the policies in the Area of freedom, security and justice should not foster the gradual move towards a surveillance society. The EDPS expects the Council to take the same approach in the Stockholm programme, also by acknowledging the orientations in point 25 hereinafter.

24. This is all the more important since the Area of freedom, security and justice is an area which 'shapes the citizens circumstances of life, in particular the private space of their own responsibility and of political and social security, which is protected by the fundamental rights', as very recently emphasised by the German Constitutional Court in its judgment of 30 June 2009 relating to the Lisbon Treaty ([13]).

([9]) The 2007 PNR Agreement mentioned in the previous footnote and its predecessors.

([10]) 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. Although the legal basis is Article 95 EC, it was an immediate reaction to the London bombings.

([11]) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60.

([12]) See the title of the Communication.

([13]) Press Release No 72/2009 of 30 June 2009 of the Federal Constitutional Court of Germany, paragraph 2c).

25. The EDPS underlines that in such an area:

— information should be exchanged between the authorities of the Member States, including where relevant European bodies or databases, on the basis of adequate and effective mechanisms that fully respect the fundamental rights of the citizen and ensure mutual trust,

— this requires not only availability of information, combined with mutual recognition of the legal systems of the Member States (and the EU), but also a harmonisation of standards of protection of information, for instance, but not solely, through a common framework of data protection,

— these common standards should not only be applicable to situations with cross-border dimensions. Mutual trust can only exist when the standards are solid, and are always respected, without a risk that they will not apply once the cross-border dimension is not or no longer evident. Apart from this, especially when it comes to the use of information, differences between 'internal' and 'cross-border' data cannot work in practice ([14]).

V. INSTRUMENTS FOR DATA PROTECTION

V.1. Towards a comprehensive data protection scheme

26. The EDPS endorses the strategic approach of giving data protection a prominent place in the Communication. Indeed, many initiatives in the Area of freedom, security and justice rely on the use of personal data, and good data protection is crucial for their success. Respect of privacy and data protection is not only a legal obligation with an increasing recognition at EU level, but is also an issue which is crucial for European citizens, as shown by the results of the Eurobarometer ([15]). Moreover, restricting access to personal data is also crucial to ensure trust by law enforcement agencies.

27. Paragraph 2.3 of the Communication states that a comprehensive data protection scheme is needed that covers all areas of EU competence ([16]). The EDPS fully supports this objective, independently of the entry into force of the Lisbon Treaty. He also notes that such a scheme does not necessarily mean one legal framework applying to all processing. Under the current treaties, the possibilities for adopting one, comprehensive legal framework applying to all processing are limited due to the pillar structure and due to the fact that — in the first pillar at least — protection of data processed by European institutions takes place on a separate legal basis (Article 286 EC). However, the EDPS points out that some improvements may be implemented by fully exploiting the possibilities offered by the current treaties, as already highlighted by the Commission in its Communication 'Implementing the Hague programme — The way forward' ([17]). After the entry into force of the Lisbon Treaty, Article 16 TFEU will provide for the necessary legal basis for one comprehensive legal framework applying to all processing.

28. The EDPS notes that it is crucial — in any event — to ensure consistency within the legal framework for data protection where necessary through harmonisation and consolidation of the various legal instruments applicable in the Area of freedom, security and justice.

Under the current treaties

29. A first step was recently taken through the adoption of Council Framework Decision 2008/977/JHA ([18]). However, this legal instrument can not be qualified as a comprehensive framework, in essence because its provisions do not have general application. They do not apply to internal situations, when personal data originate from the Member State which uses them. Such a limitation is bound to diminish the added value of the Council Framework Decision, unless all the Member States would decide to include the internal situations in the national implementing legislation which is not likely to happen.

30. A second reason why the EDPS considers that in the long run the Council Framework Decision 2008/977/JHA does not contain a satisfactory data protection framework in an area of freedom, security and justice is that several essential provisions are not in line with Directive 95/46/EC. Under the current treaties, a second step could be set by widening the scope and aligning the Council Framework Decision to Directive 95/46/EC.

31. Another impetus to the realisation of a comprehensive data protection scheme could be given by establishing a clear and long-term vision. This vision could contain a global and coherent approach to define collection and exchanges of data — as well as the exploitation of existing databases

([14]) The EDPS has elaborated this last point in his Opinion of 19 December 2005 on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final), OJ C 47, 25.2.2006, p. 27, paragraphs 30-32.

([15]) Data Protection in the European Union — Citizens' perceptions — Analytical report, Flash Eurobarometer Series 225, January 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) See also the priority issues of the Communication.

([17]) COM(2006) 331 final of 28 June 2006.

([18]) See footnote 11.

— and at the same time the data protection guarantees. This vision should prevent useless overlapping and duplication of instruments (and thus of processing of personal data). It should also foster the consistency of the EU policies in this area as well as the trust about how public authorities handle citizen data. The EDPS recommends Council to announce the need for a clear and long-term vision in the Stockholm programme.

32. A further recommendation of the EDPS is to evaluate and put into perspective the measures that have already been adopted in this area, their concrete implementation and their effectiveness. This evaluation should duly take into account the costs for privacy and the effectiveness for law enforcement. Should these evaluations prove that certain measures do not deliver the results envisaged or are not proportionate to the purposes pursued, the following steps should be considered:

— as a first step, amending or repealing the measures insofar as they do not appear to be sufficiently justified in generating a concrete added value for law enforcement authorities and for European citizens,

— as a second step, assessing the possibilities for improving the application of the existing measures,

— only as a third step, proposing new legislative measures if it is probable that those new measures are needed for the purposes envisaged. New instruments should only be adopted if they have a clear and concrete added value for law enforcement authorities and for European citizens.

The EDPS recommends making a reference to a system of evaluation of existing measures in the Stockholm programme.

33. Last but not least, special emphasis should be put on the better implementation of existing safeguards, in line with the Commission Communication on the follow-up of the Work Programme for better implementation of the Data Protection Directive ([19]) and the suggestions made by the EDPS in his opinion on that Communication ([20]). Unfortunately, in the third pillar the Commission lacks the possibility of starting infringement procedures.

Under the Lisbon Treaty

34. The Lisbon Treaty opens up for a genuine comprehensive data protection framework. Article 16.2 of the Treaty on the functioning of the European Union requires from Council and European Parliament to lay down the rules relating to data protection by Union institutions, bodies, offices and agencies, by the Member States when carrying out activities which fall within the scope of Union law, and by private parties.

35. The EDPS understands the emphasis of the Communication on a comprehensive data protection scheme as an ambition of the Commission to propose a legal framework which applies to all processing activities. He fully endorses this ambition, which enhances the consistency of the system, ensures legal certainty and by doing so improves the protection. In particular, it would avoid in the future the difficulties of finding a dividing line between the pillars when data collected in the private sector for commercial purposes are later on used for law enforcement purposes. This dividing line between the pillars does not fully reflect reality, as the important judgments of the Court of Justice in PNR ([21]) and in data retention ([22]) prove.

36. The EDPS suggests emphasising this rationale of a comprehensive data protection scheme in the Stockholm programme. It shows that such a scheme is not just a simple preference but is a necessity due to the changing practices in data use. He recommends including as a priority in the Stockholm-programme the need for a new legislative framework, inter alia, replacing Council Framework Decision 2008/977/JHA.

37. The EDPS underlines that the notion of a comprehensive data protection scheme based on a general legal framework does not exclude the adoption of additional rules for data protection for the police and the judicial sector. Those additional rules could take into account the specific needs for law enforcement, as foreseen by Declaration 21, attached to the Lisbon Treaty ([23]).

V.2. **Restating data protection principles**

38. The Communication notes the technological changes transforming the communication between individuals and public and private organisations. This calls according to the Commission for restating a number of basic principles of data protection.

([19]) COM(2007) 87 final of 7 March 2007.

([20]) Opinion of 25 July 2007, OJ C 255, 27.10.2007, p. 1, in particular paragraph 30.

([21]) Judgment of the Court of 30 May 2006, European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), joined cases C-317/04 and C-318/04, ECR (2006), p. I-4721.

([22]) Judgment of the Court of 10 February 2009, Ireland v European Parliament and Council of the European Union, Case C-301/06, not yet released.

([23]) See Declaration 21 on the protection of personal data in the field of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference that adopted the Treaty of Lisbon, OJ C 115, 9.5.2008, p. 345.

39. The EDPS welcomes these intentions of the Communication. An evaluation of the effectiveness of these principles in the perspective of technological changes is extremely useful. As a first point, it is important to note that restating and reaffirming data protection principles must not always be directly related to technological developments. It could also be needed in the light of other perspectives, mentioned in Part III above, the internationalisation, the growing use of data for law enforcement and the free movement.

40. Moreover, in the view of the EDPS, this evaluation can be included in the public consultation that was announced by the Commission in the Conference 'Personal data — more use, more protection' on 19 and 20 May 2009. This public consultation could give valuable input ([24]). The EDPS suggests emphasising the link between the intentions of the Communication in paragraph 2.3 and the public consultation on the future of data protection, by the Council in the text of the Stockholm programme and by the Commission in its public statements on the consultation.

41. As an illustration of what such evaluation could cover, the following points are mentioned:

— personal data in the area of FSJ are likely to be of an especially sensitive nature, such as data relating to criminal convictions, police data and biometric data such as fingerprints and DNA profiles,

— their processing may entail negative consequences for the data subjects, especially when considering the coercive powers of law enforcement authorities. Moreover, data monitoring and analysis is increasingly automated, quite often without human intervention. Technology allows use of databases with personal data for general searches (data mining, profiling, etc.). Legal obligations on which data processing is based should be clearly laid down,

— a cornerstone of data protection law is that personal data shall be collected for specified purposes and not used in a way incompatible with those purposes. Use for incompatible purposes should only be allowed insofar as it is laid down by law and necessary to pursue specific public interests, as those laid down by Article 8.2 ECHR,

— the need to respect the purpose limitation principle might have consequences for current trends in data use. Law enforcement uses data which were collected by private companies for commercial purposes, in the telecommunications, transport and financial sectors. Furthermore, large-scale information systems are set up, for example in the areas of immigration and borders control. Moreover, interconnections and accesses to databases are allowed, thus expanding the purposes for which personal data were originally collected. A reflection on these current trends is needed, including any possible adjustments and/or additional safeguards, where required,

— in addition to the principles of data protection mentioned in the Communication, the evaluation should pay attention to the need for transparency of the processing, allowing the data subject to exercise his rights. Transparency is an especially difficult issue in the law enforcement area, in particular since transparency should be weighed against risks for the investigations,

— solutions should be found for the exchanges with third countries.

42. This evaluation should furthermore focus on the possibilities for improving the effectiveness of the application of data protection principles. In this context, it could be useful to concentrate on instruments that can reinforce the responsibilities of the data controllers. These instruments must allow full accountability of the data controllers for data management. 'Data governance' is a useful notion in this context. This covers all legal, technical and organisational means by which organisations ensure full responsibility over the way in which data are handled, such as planning and control, use of sound technology, adequate training of staff, compliance audits, etc.

V.3. **Privacy-aware technologies**

43. The EDPS is glad that paragraph 2.3 of the Communication mentions privacy certification. In addition to this, reference could be made to 'privacy by design' and the need to identify 'Best Available Techniques' compliant to the data protection framework of the EU.

44. In the view of the EDPS, 'privacy by design' and privacy-aware technologies, could be helpful tools for a better protection, as well as for a more effective use of information. The EDPS suggests two — not mutually exclusive — ways forward:

— a privacy and data protection certification scheme ([25]) as option for builders and users of information systems, either or not supported by EU funding or EU legislation,

([24]) The Article 29 Working Party on Data Protection, in which the EDPS participates, has decided to work intensively on its contribution to this public consultation.

([25]) An example of such a scheme is the European Privacy Seal (EuroPriSe).

— a legal obligation for builders and users of information systems to use systems which are in accordance with the principle of privacy by design. This might require enlarging the present scope of data protection law to make builders responsible for the information systems they develop ([26]).

The EDPS suggests mentioning these possible ways forward in the Stockholm programme.

V.4. **External aspects**

45. Another subject mentioned in the Communication is the development and promotion of international standards for data protection. Presently, many activities take place in view of the establishment of feasible standards for global application, for instance by the International Conference of Privacy and Data Protection Commissioners. In the near future, this might lead to an international agreement. The EDPS suggests that the Stockholm programme supports these activities.

46. The Communication also mentions the conclusion of bilateral agreements, based on the progress already made together with the United States. The EDPS shares the need for a clear legal framework for transferring data to third countries, and thus welcomed the joint work of the EU and the US authorities in the High-Level Contact Group on a possible transatlantic instrument on data protection, while calling for more clarity and attention to specific issues ([27]). In this perspective, it is also interesting to note the ideas in the Home Affairs Report for a Euro-Atlantic Area of cooperation in freedom, security, justice on which, according to this report, the EU should decide by 2014. Such area would not be possible without proper guarantees on data protection.

47. According to the EDPS, the European standards for data protection, based on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data ([28]) and the case law of the European Court of Justice and the European Court for Human Rights, should determine the level of protection in a general agreement with the United States on data protection and data exchange. Such a general agreement could be the basis for specific arrangements for the exchange of personal data. This is even more important in the light of the intention formulated in paragraph 4.2.1 of the Communication that the European Union must conclude police cooperation agreements wherever necessary.

48. The EDPS fully understands the need of enhancing international cooperation, in some cases also with countries not protecting fundamental rights. However ([29]), it is crucial to take into account that this international cooperation is likely to generate a large increase in the collection and international transfer of data. Therefore, it is essential that principles of fair and lawful processing — as well as principles of due process in general — apply to the collection and transfer of personal data across Union borders, and that personal data are transferred to third countries or international organisations only if an adequate level of protection or other appropriate safeguards are guaranteed by those third parties concerned.

49. To conclude, the EDPS recommends emphasising in the Stockholm programme the importance of general agreements with the United States and other third countries on data protection and data exchange, based on the level of protection guaranteed within the territory of the EU. In a broader perspective, the EDPS points at the importance of actively promoting the respect of fundamental rights, and in particular of data protection, in relation with third countries and with international organisations ([30]). Furthermore, the Stockholm programme could mention the general notion that exchange of personal data with third countries requires an adequate level of protection or other appropriate safeguards in those third countries.

VI. **THE USE OF INFORMATION**

VI.1. **Towards a European information model**

50. A better exchange of information is an essential policy goal for the European Union, in the Area of freedom, security and justice. Paragraph 4.1.2 of the Communication emphasises that security in the European Union depends on effective mechanisms for exchanging information between national authorities and other European players. This emphasis on information exchange is logical, in the absence of a European police force, a European criminal justice system and a European border control. Measures

([26]) Users of information are covered by data protection law, as data controllers or processors.

([27]) See EDPS Opinion of 11 November 2008 on the Final Report by the EU-US High-Level Contact Group on information sharing and privacy and personal data protection, OJ C 128, 6.6.2009, p. 1.

([28]) ETS No 108, 28.1.1981.

([29]) See letter EDPS of 28 November 2005 on the Commission communication on the external dimension of the Area of freedom, security and justice available at the EDPS website.

([30]) The recent case law on terrorists' lists confirms that guarantees are needed — also in the relations with the United Nations — in order to ensure that counterterrorism measures comply with EU standards on fundamental rights (joined Cases C-402/05 P and C-415/05 P, Kadi and Al Barakaat Foundation v Council, judgment of 3 September 2008, not yet released).

relating to information are therefore essential contributions of the European Union allowing the authorities of the Member States to address cross-border crime in an effective way and to effectively protect the external borders. However, they do not only contribute to the security of the citizens but also to their freedom — the free movement of persons was mentioned before as a perspective of this opinion — and to justice.

51. It is precisely for these reasons that the principle of availability was introduced in the Hague programme. It entails that information needed for the fight against crime should cross the internal borders of the EU without obstacles. Recent experiences show that it was difficult to implement this principle into legislative measures. The Commission proposal for a Council framework decision on the exchange of information under the principle of availability of 12 October 2005 ([31]) was not accepted in the Council. The Member States were not ready to accept the consequences of the principle of availability to its full extent. Instead, more limited instruments ([32]) were adopted such as the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime ('Prüm-decision') ([33]).

52. While the principle of availability was at the core of the Hague programme, the Commission now seems to take a more modest approach. It envisages further stimulating the exchange of information between authorities of the Member States by introducing the European information model. The Swedish EU presidency thinks in the same line ([34]). It will present a proposal for a strategy for the exchange of information. The Council already started its work on this ambitious project of a European Union Information Management Strategy, which is closely linked to the European information model. The EDPS notes these developments with great interest and underlines the attention that should be given in these projects to data protection elements.

A European information model and data protection

53. As a starting point, it should be emphasised that the future of the Area of freedom, security and justice should not be 'technology-driven', in the sense that the almost limitless opportunities offered by new technologies should always be checked against relevant data protection principles and used only insofar as they comply with those principles.

54. The EDPS notes that the Communication presents the information model not only as a technical model: a powerful strategic analysis capacity and better gathering and processing of operational information. It also acknowledges that policy related aspects — like criteria for gathering, sharing and processing of information — should be taken into account, while complying with data protection principles.

55. Information technology and legal conditions are — and will continue to be — both essential. The EDPS welcomes the Communication that starts from the assumption that a European information model may not be construed on the basis of technical considerations. It is essential that information is gathered, shared and processed only on the basis of concrete needs for security and taking into account data protection principles. The EDPS also fully subscribes the need for defining a follow up mechanism for assessing how the exchange of information operates. He suggests that the Council further elaborates these elements in the Stockholm programme.

56. In this context, the EDPS underlines that data protection, aiming to protect the citizen, should not be seen as hampering effective data management. It provides important tools to improve the storage, access and exchange of information. The rights of the data subject to be informed about which information concerning him or her is processed and to rectify incorrect information can also strengthen the accuracy of data in data management systems.

57. Data protection law has in essence the following consequences: if data are needed for a specific and legitimate purpose they can be used; if they are not needed for a well-defined purpose, personal data should not be used. In the first case, it may well take additional measures to provide adequate safeguards.

58. The EDPS however is critical to the extent in which the Communication mentions the 'identification of future needs' as part of the information model. He emphasises that also in the future the purpose limitation principle should be guiding when building information systems ([35]). It is one of the essential guarantees that the data protection system gives to the citizen: he must be able to know in advance for what purpose data relating to him are collected and that it will be used only for that purpose, notably in the future. This guarantee is even enshrined in Article 8 of the Charter of the Fundamental Rights of the Union. The purpose limitation principle allows exceptions — which are in particular relevant in the Area of freedom, security and justice — but those exceptions should not determine the construction of a system.

([31]) COM(2005) 490 final.
([32]) In the perspective of availability; the Prüm Decision contains far reaching provisions for the use of biometric data (DNA and fingerprints).
([33]) OJ L 210, 6.8.2008, p. 1.
([34]) See the governments' EU Work programme cited in footnote 5, p. 23.
([35]) See also point 41 above.

Choosing the right architecture

59. Choosing the right architecture for information exchange is the start of it all. The importance of proper information architectures is recognised in the Communication (paragraph 4.1.3) but unfortunately only in relation to interoperability.

60. The EDPS stresses another aspect: within the European information model, data protection requirements should be an integral part of all system development and should not just be seen as a necessary condition for the legality of a system ([36]). Use should be made of the concepts of 'privacy by design' and need to identify 'Best Available Techniques' ([37]), as introduced in point 43 above. The European information model should build on these concepts. This means, more concretely, that information systems which are designed for purposes of public security should always be built in accordance with the principle of 'privacy by design'. The EDPS recommends the Council to include these elements in the Stockholm programme.

Interoperability of systems

61. The EDPS underlines that interoperability is not a purely technical issue but also has consequences for the protection of the citizen, in particular data protection. From the perspective of data protection, interoperability of systems, if done well, has clear advantages in terms of avoiding double storage. However, it is also obvious that making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data. In other words, interoperability has particular risks of interconnection between databases having different purposes ([38]). It can affect the strict limitations on the purpose of databases.

62. In short, the mere fact that it is technically possible to exchange digital information between interoperable databases or to merge these databases does not justify an exception to the purpose limitation principle. Interoperability should in concrete cases be based on clear and careful policy choices. The EDPS suggests specifying this notion in the Stockholm programme.

VI.2. **The use of information collected for other purposes**

63. The Communication does not explicitly address one of the most important tendencies of the recent years, namely the use for law enforcement purposes of data collected in the private sector for commercial purposes. This tendency does not only relate to the traffic data of electronic communications and the passenger data of individuals flying to (certain) third countries ([39]) but also focuses on the financial sector. An example is Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing ([40]). Another well known and much debated example concerns the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) ([41]) of data which are necessary for the purpose of the US Treasury Department's Terrorist Finance Tracking Programme.

64. The EDPS considers that these tendencies require specific attention in the Stockholm programme. They can be seen as derogations from the purpose limitation principle and are often very privacy-intrusive since the use of these data can reveal a lot about the behaviour of individuals. In each case where such measures are proposed, there must be very strong evidence that such an intrusive measure is needed. If this evidence is given, it must be ensured that rights of individuals are fully safeguarded.

65. According to the EDPS the use for law enforcement of personal data collected for commercial purposes should only be allowed under strict conditions, such as:

— data are only used for specifically defined purposes such as the fight against terrorism or serious crime, to be determined on a case-by-case basis,

— data are transferred through a 'push' rather than a 'pull' system ([42]),

([36]) See 'Guidelines and criteria for the development, implementation and use of privacy enhancing security technologies' developed in the PRISE project (http://www.prise.oeaw.ac.at).

([37]) Best Available Techniques shall mean the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for ITS applications and systems to be compliant with privacy, data protection and security requirement of the EU regulatory framework.

([38]) See EDPS Comments on the Communication of the Commission on interoperability of European databases, 10 March 2006, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) See e.g. point 15 above.

([40]) OJ L 309, 25.11.2005, p. 15.

([41]) See Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) of the Article 29 Working Party.

([42]) Under the 'push' system the data controller sends the data on request (pushes) to the law enforcement agency. Under the 'pull' system the law enforcement agency has access to the database of the controller and extracts (pulls) information from this database. Under the 'pull' system it is more difficult for the controller to resume its responsibility.

— requests for data should be proportionate, narrowly targeted and, in principle, based on suspicions on specific persons,

— routine searches, data mining and profiling should be avoided,

— all use of the data for law enforcement purposes should be logged in order to allow effective control on the use, by the data subject exercising his rights, by data protection authorities and by the judiciary.

VI.3. **Information systems and EU bodies**

Information systems with or without centralised storage ([43])

66. Over the last years, the number of information systems based on EU law has significantly grown within the Area of freedom, security and justice. Sometimes decisions are made to establish a system which entails centralised storage of data on the European level, in other cases the law only foresees exchange of information between national databases. The Schengen Information System is probably the best example of a system with centralised storage. Council Decision 2008/615/JHA (Prüm-decision) ([44]) is from the perspective of data protection the most significant example of a system without centralised storage since it foresees a massive exchange of biometric data between the authorities in the Member States.

67. The Communication illustrates that this tendency of creating new systems will continue. A first example, taken from paragraph 4.2.2 is an information system expanding the European Criminal Records Information System (ECRIS) to cover nationals of non-EU countries. The Commission already commissioned a study on the European Index for Convicted Third Country Nationals (EICTCN), possibly leading to a centralised database. A second example is the exchange of information of individuals in insolvency registers in other Member States, in the frame of e-Justice (paragraph 3.4.1 of the Communication) without centralised storage.

68. A decentralised system would have certain advantages from the perspective of data protection. It avoids double storage of data by the authority of the Member State and by the centralised system, the responsibility for the data is clear since the authority of the Member State will be the controller, and control by the judiciary and by data protection authorities can take place on Member States level. But this system also has weaknesses when data are exchanged with other jurisdictions, for instance in ensuring that information is kept up to date both in the country of origin and the country of destination and how to ensure effective control on both sides. It is even more complicated to ensure responsibility for the technical system for the exchange. These weaknesses can be overcome by choosing for a centralised system with a responsibility for European bodies at least for parts of the system (such as the technical infrastructure).

69. In this context, it would be useful to develop substantive criteria for the choice between centralised and decentralised systems, ensuring clear and careful policy choices in concrete cases. These criteria can contribute to the functioning of the systems themselves, as well as to the protection of the citizen's data. The EDPS suggests including the intention of developing such criteria in the Stockholm programme.

Large-scale information systems

70. Paragraph 4.2.3.2 of the Communication briefly discusses the future of the large-scale information systems with an emphasis on the Schengen Information System (SIS) and the Visa Information System (VIS).

71. Paragraph 4.2.3.2 also mentions the establishment of an electronic system for entry to and exit from Member States' territory alongside registered traveller programmes. This system was announced earlier by the Commission as part of the 'borders package' on the initiative of Vice-President Frattini ([45]). In his preliminary comments ([46]), the EDPS was fairly critical about this proposal because the need for such an intrusive system, on top of existing large-scale systems was not sufficiently demonstrated. The EDPS does not notice any additional evidence of the need for such a system and therefore suggests to the Council not to mention this idea in the Stockholm programme.

72. In this context, the EDPS wishes to refer to his opinions on various initiatives in the field of EU information exchange ([47]) in which he made numerous suggestions and comments on the data protection implications of the use of the large databases at EU level. Amongst other issues, he paid particular attention to the need for strong and tailor-made safeguards that should be in place as well

([43]) Centralised storage is in this context understood as storage on a central European level, whereas decentralised storage means storage on the level of the Member States.

([44]) See footnote 33.

([45]) Communication of the Commission 'Preparing the next steps in border management in the European Union', 13.2.2008, COM(2008) 69.

([46]) Preliminary comments EDPS on three communications from the Commission on border management (COM(2008) 69, COM(2008) 68 and COM(2008) 67), 3 March 2008: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) In particular: Opinion 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, OJ C 181, 23.7.2005, p. 13, and Opinion of 19 October 2005 on three proposals regarding the second generation Schengen Information System (SIS II), OJ C 91, 19.4.2006, p. 38.

as the proportionality and necessity of impact assessments before any measures are proposed or undertaken in this area. The EDPS has always advocated a right and data protection compliant balance between security requirements and the protection of privacy of individuals subject to the systems. He took the same position when acting as the supervisor of the central parts of the systems.

73. Furthermore, the EDPS takes this opportunity to emphasise the need for a consistent approach to the EU information exchange as a whole, in terms of legal, technical and supervisory consistency between the systems already in place and those which are being developed. Indeed, nowadays, more than before, there is a clear need for a courageous and comprehensive vision on how the EU information exchange and the future of large-scale information systems should look like. Only on the basis of such a vision, an electronic system for entry to and exit from Member States' territory could possibly be reconsidered.

74. The EDPS suggests referring in the Stockholm programme to the intention to develop such a vision, which should include a reflection on the possible entry into force of the Lisbon Treaty and its implications on the systems based on a first and third pillar legal basis.

75. Finally, the Communication mentions the setting up of a new agency which according to the Communication should also become competent for the electronic entry and exit system. In the meantime, the Commission adopted a proposal for the setting up of such an agency ([48]). The EDPS supports this proposal in principle since it can make the functioning of these systems, including data protection more effective. He will present an opinion on this proposal in due time.

Europol and Eurojust

76. The role of Europol is mentioned at several places in the Communication which emphasises as a priority issue that Europol must play a central role in coordination, exchange of information, and training of professionals. Equally, paragraph 4.2.2 of the Communication refers to the recent changes in the legal framework of cooperation between Eurojust and Europol and announces that work will continue on strengthening Eurojust, particularly as regards investigations into areas of cross-border organised crime. The EDPS fully supports these objectives, provided that safeguards for data protection are respected in an appropriate way.

77. In this context, the EDPS welcomes the new draft agreement recently reached between Europol and Eurojust ([49]), which aims at improving and enhancing mutual cooperation between the two bodies and providing for efficient exchange of information between them. This is a work in which efficient and effective data protection plays a crucial role.

VI.4. **The use of biometric data**

78. The EDPS notes that the Communication does not address the issue of the increasing use of biometric data in different legal instruments of the European Union on the use of information exchange, including the instruments establishing the large-scale information systems. This is regrettable given that it is a matter of particular importance and sensitivity from the perspectives of data protection and privacy.

79. Although the EDPS recognises the general advantages of the use of biometrics, he has been constantly stressing the major impacts of the use of such data on individuals' rights and has been suggesting the insertion of stringent safeguards for the use of biometrics in each particular system. The recent judgment of the European Court of Human Rights in S. and Marper v the United Kingdom ([50]) provides useful indications in this context, in particular on the justification and the limits of the use of biometric data. In particular the use of DNA information can reveal sensitive information about individuals, also taking into account that the technical possibilities of extracting information from DNA are still growing. In the case of large-scale use of biometric data in information systems, there is also a problem due to inherent inaccuracies in the collection and comparison of biometric data. For these reasons, the EU legislator should show restraint with the use of these data.

80. Another recurring issue in recent years has been the use of fingerprints of children and of elderly people, because of the inherent imperfections of biometric systems for those age groups. The EDPS asked for an in-depth study in order to identify properly the accuracy of the systems ([51]). He proposed an age limit of 14 years for children, unless this study proves otherwise. The EDPS recommends mentioning this issue in the Stockholm programme.

([48]) Commission proposal of 24 June 2009 for a regulation of the European Parliament and of the Council establishing an Agency for the operational management of the Schengen Information System (SIS II), Visa Information System (VIS), EURODAC and other large-scale IT systems in the Area of freedom, security and justice (COM(2009) 293/2).

([49]) Draft agreement, approved by Council, and still to be signed by both parties. See Council register:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Joined applications 30562/04 and 30566/04, S. and Marper v United Kingdom, judgment of 4 December 2008, ECHR not yet released.

([51]) Opinion of 26 March 2008 on the proposal for a regulation amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ C 200, 6.8.2008, p. 1.

81. Having said this, the EDPS suggests it would be useful to develop substantive criteria for the use of biometric data. Those criteria should ensure that the data are only used when necessary, adequate and proportionate, and when an explicit, specified and legitimate purpose has been demonstrated by the legislator. To be more specific, biometric data and in particular DNA data should not be used if the same effect can be reached by using other, less sensitive information.

VII. **ACCESS TO JUSTICE AND E-JUSTICE**

82. Technology will also be used as a tool for better judicial cooperation. In paragraph 3.4.1 of the Communication, e-Justice is presented as providing the citizens easier access to justice. It consists of a portal with information and video-conferences as part of the legal procedure. It furthermore opens up for online legal procedures and it foresees the interconnection of national registers, such as insolvency registers. The EDPS notes that the Communication does not mention new initiatives about e-Justice but consolidates actions that are already set in motion. The EDPS is involved in some of these actions, as a follow up of the Opinion he issued on 19 December 2008 on the Communication from the Commission towards a European e-Justice Strategy ([52]).

83. e-Justice is an ambitious project that needs full support. It can effectively improve the justice system in Europe and the judicial protection of the citizen. It is a significant step forward towards a European Area of Justice. Keeping this positive appreciation in mind, a few remarks can be made:

— the technological systems for e-Justice should be built in accordance with the principle of 'privacy by design'. As said before, in relation to the European information model, choosing the right architecture is the start of it all,

— the interconnection and interoperability of systems should respect the purpose limitation principle,

— the responsibilities of the different actors should be precisely defined,

— the consequences for individuals of the interconnection of national registers with delicate personal data, such as insolvency registers, should be analysed in advance.

VIII. **CONCLUSIONS**

84. The EDPS endorses the emphasis in the Communication on the protection of fundamental rights, and in particular the protection of personal data, as one of the key issues of the future of the Area of freedom, security and justice. In the view of the EDPS, the Communication rightly promotes a balance between the needs for appropriate instruments to guarantee the security of the citizen and the protection of their fundamental rights. It recognises that more emphasis should be given to the protection of personal data.

85. The EDPS fully supports paragraph 2.3 of the Communication that calls for a comprehensive data protection scheme covering all areas of EU competence, independently of the entry into force of the Lisbon Treaty. He recommends in this context:

— to announce the need for a clear and long-term vision on such a comprehensive scheme, in the Stockholm-programme,

— to evaluate the measures that have been adopted in this area, their concrete implementation and their effectiveness, taking into account the costs for privacy and the effectiveness for law enforcement,

— to include as a priority in the Stockholm programme, the need for a new legislative framework, inter alia, replacing Council Framework Decision 2008/977/JHA.

86. The EDPS welcomes the intentions of the Commission to reaffirm the data protection principles, which must be connected to the public consultation announced by the Commission in the Conference 'Personal data — more use, more protection?' on 19 and 20 May 2009. On substance, the EDPS emphasises the importance of the purpose limitation principle as a cornerstone of data protection law, and of focusing on the possibilities for improving the effectiveness of the application of data protection principles, by instruments that can reinforce the responsibilities of the data controllers.

87. 'Privacy by design' and privacy-aware technologies, could be promoted by:

— a privacy and data protection certification scheme as option for builders and users of information systems,

— a legal obligation for builders and users of information systems to use systems which are in accordance with the principle of 'privacy by design'.

88. As to the external aspects of data protection, the EDPS recommends:

— emphasising in the Stockholm programme the importance of general agreements with the United States and other third countries on data protection and data exchange,

([52]) EDPS Opinion of 19 December 2008 on the Communication from the Commission towards a European e-Justice Strategy, OJ C 128, 6.6.2009, p. 13.

— actively promoting the respect of fundamental rights, and in particular of data protection, in relation with third countries and with international organisations,

— mentioning in the Stockholm programme that exchange of personal data with third countries requires an adequate level of protection or other appropriate safeguards in those third countries.

89. The EDPS notes the developments towards a European Union Information Management Strategy and a European information model with great interest and underlines the attention that should be given in these projects to data protection elements, to be further elaborated in the Stockholm programme. The architecture for information exchange should be based on 'privacy by design' and 'Best Available Techniques'.

90. The mere fact that it is technically possible to exchange digital information between interoperable databases or to merge these databases does not justify an exception to the purpose limitation principle. Interoperability should in concrete cases be based on clear and careful policy choices. The EDPS suggests specifying this notion in the Stockholm programme.

91. The use for law enforcement of personal data collected for commercial purposes should, according to the EDPS, only be allowed under strict conditions, specified in point 65 of this opinion.

92. Other suggestions as to the use of personal information include:

— develop substantive criteria for the choice between centralised and decentralised systems, and include the intention of developing such criteria in the Stockholm programme,

— the establishment of an electronic system for entry to and exit from Member States' territory alongside registered travellers programmes should not be mentioned in the Stockholm programme,

— support for the strengthening of Europol and Eurojust and for the new agreement recently elaborated between Europol and Eurojust,

— develop substantive criteria for the use of biometric data, ensuring that the data are only used when necessary, adequate and proportionate, and when an explicit, specified and legitimate purpose has been demonstrated by the legislator. DNA data should not be used if the same effect can be reached by using other, less sensitive information.

93. The EDPS supports e-Justice and has made a few remarks on how to improve the project (see point 83).

Done at Brussels, 10 July 2009.

Peter HUSTINX

European Data Protection Supervisor