ISSN 1725-2423

Official Journal of the European Union

C 128

English edition

Information and Notices

Volume 52

6 June 2009

Notice No | Contents | Page

EN

(Continued overleaf)

EN

I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection

(2009/C 128/01)

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,

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 — CONTEXT OF THE OPINION

1. On 28 May 2008, the Presidency of the Council of the European Union announced to the COREPER, in the perspective of the EU summit of 12 June 2008, that the EU-US High Level Contact Group (hereafter HLCG) on information sharing and privacy and personal data protection had finalised its report. This report was made public on 26 June 2008 ([1]).

2. The report tends to identify common principles for privacy and data protection as a first step towards exchange of information with the United States to fight terrorism and serious transnational crime.

3. In its announcement, the Presidency of the Council states that it would welcome any ideas with regard to the follow-up to this report, and in particular reactions to the recommendations on the ways forward identified in the report. The EDPS answers to this invitation by issuing the following opinion, based on the state of play as made public and without prejudice to any further position he might take considering the evolution of the issue.

4. The EDPS notes that the work of the HLCG has taken place in a context that has seen, especially since 11 September 2001, the development of exchange of data between the US and the EU, through international agreements or other types of instruments. Among them are the agreements of Europol and Eurojust with the United States, and also the PNR agreements and the Swift case which led to an exchange of letters between EU and US officials to establish minimal data protection guarantees ([2]).

([1]) Council Document No 9831/08, available at: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Agreement between the United States of America and the European Police Office of 6 December 2001, and Supplemental agreement between Europol and the USA on exchange of personal data and related information, published on the website of Europol;
— Agreement between the United States of America and Eurojust on judicial cooperation of 6 November 2006, published on the website of Eurojust;
— 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), signed in Brussels, 23 July 2007 and in Washington, 26 July 2007, OJ L 204, 4.8.2007, p. 18;
— Exchange of letters between the US and EU authorities on the Terrorist Finance Tracking Program, 28 June 2007.

5. Furthermore, the EU also negotiates and agrees to similar instruments providing for the exchange of personal data with other third countries. A recent example is the Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service ([3]).

6. It appears from this context that the request of enforcement authorities of third countries for personal information is constantly widening, and that it also extends from traditional government data bases to other types of files, in particular files of data collected by the private sector.

7. As an important background element, the EDPS also recalls that the issue of transfer of personal data to third countries in the framework of police and judicial cooperation in criminal matters is addressed in the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters ([4]) that is likely to be adopted before the end of 2008.

8. This transatlantic exchange of information can only be expected to grow and to touch additional sectors where personal data are being processed. In such a context, a dialogue on 'transatlantic law enforcement' is at the same time welcome and sensitive. It is welcome in the sense that it could give a clearer framework to the exchanges of data that are or will be taking place. It is also sensitive since such a framework could legitimise massive data transfers in a field — law enforcement — where the impact on individuals is particularly serious, and where strict and reliable safeguards and guarantees are all the more needed ([5]).

9. This Opinion will in the following chapter address the current state of play and the possible ways forward. Chapter III will focus on the scope and nature of an instrument that would allow for information sharing. In Chapter IV, the opinion will analyse from a general perspective legal issues linked with the content of a possible agreement. It will address issues like the conditions of assessment of the level of protection provided in the United States, and will discuss the question of the use of the EU regulatory framework as a benchmark in order to assess this level of protection. This chapter will also list the basic requirements to be included in such an agreement. Finally, in Chapter V the opinion will provide for an analysis of the privacy principles attached to the report.

([3]) OJ L 213, 8.8.2008, p. 49.

([4]) Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, version of 24 June 2008 available at http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) As to the necessity of a clear legal framework, see Chapters III and IV of this Opinion.

II. THE CURRENT STATE OF PLAY AND POSSIBLE WAYS FORWARD

10. The EDPS evaluates the current state of play as follows. Some progress has been made towards the definition of common standards on information sharing and privacy and personal data protection.

11. However, preparatory work for any type of agreement between the EU and the US is not yet finished. Additional work is needed. The report of the HLCG itself mentions a number of outstanding issues of which the issue of 'redress' is the most prominent. Disagreement remains over the necessary scope of judicial redress ([6]). Five other outstanding issues have been identified in Chapter 3 of the Report. It follows furthermore from this Opinion that many other questions are not yet solved, for instance on the scope and nature of an instrument on information sharing.

12. Since the preferred option of the report is a binding agreement — the EDPS shares this preference — prudence is all the more required. Further careful and in depth preparations are needed before an agreement can be achieved.

13. Finally, according to the EDPS, the conclusion of an agreement should best take place under the Lisbon Treaty, of course depending on its entry into force. Indeed, under the Lisbon Treaty no legal uncertainty about the dividing line between the pillars of the EU would arise. Moreover, full involvement of the European Parliament would be guaranteed as well as judicial control by the Court of Justice.

14. Under those circumstances, the best way forward would be the development of a road map towards a possible agreement at a later stage. Such a road map could contain the following elements:

— Guidance for the continuation of the work of the HLCG (or any other group) as well as a timeline.

— At an early stage, discussion and possibly agreement on fundamental issues like scope and nature of the agreement.

— On the basis of a common understanding of these fundamental issues, further elaboration of the data protection principles.

— Involvement of stakeholders at different stages of the procedure.

— On the European side, addressing the institutional constraints.

([6]) Page 5 of the report, under C.

III. SCOPE AND NATURE OF AN INSTRUMENT ON INFORMATION SHARING

15. It is crucial in the view of the EDPS that the scope and the nature of a possible instrument including data protection principles are clearly defined, as a first step of the further development of such an instrument.

16. As to the scope, important questions to be answered are:

— who are the actors involved, within and outside the law enforcement area,

— what is intended by the 'purpose of law enforcement', and its relation to other purposes such as national security, and more specifically border control and public health,

— how the instrument would fit in the perspective of a global transatlantic security area.

17. The definition of the nature should clarify the following issues:

— if relevant, under which pillar the instrument will be negotiated,

— whether the instrument will be binding on the EU and the US,

— whether it will have direct effect, in the sense that it contains rights and obligations for individuals that can be enforced before a judicial authority,

— whether the instrument itself will allow for the exchange of information or will set a minimum-standard for the exchange of information to be complemented by specific agreements,

— how the instrument will relate to existing instruments: will it respect, replace or complement them?

III.1. Scope of the instrument

Actors involved

18. Although there is no clear indication in the report of the HLCG on the precise scope of the future instrument, it can be deduced from the principles mentioned therein that it envisages covering both transfers between private and public actors ([7]) and between public authorities.

— Between private and public actors:

19. The EDPS sees the logic of the applicability of a future instrument to transfers between private and public actors. The development of such an instrument takes place against the background of requests from the US side for information from private parties in recent years. The EDPS notes indeed that private actors are becoming a systematic source of information in a law enforcement perspective, be it at the level of the EU or at international level ([8]). The SWIFT case was a major precedent where a private company was requested to systematically transmit data in bulk to law enforcement authorities of a third state ([9]). The collection of PNR data from airlines follows the same logic. In his opinion on a draft framework decision for a European PNR system, the EDPS has already questioned the legitimacy of this trend ([10]).

20. There are two more reasons to be reluctant about the inclusion of transfers between private and public actors within the scope of a future instrument.

21. In the first place, inclusion could have an unwanted effect within the territory of the EU itself. The EDPS has serious concerns that if data of private companies (like financial institutions) can be transferred to third countries in principle, this could provoke a strong pressure to make the same type of data equally available within the EU to law enforcement authorities. The PNR scheme is an example of such unwelcome development, which started by a bulk collection of passenger data by the US, to be then transposed to the internal European context as well ([11]) without that the necessity and proportionality of the system have been clearly demonstrated.

22. In the second place, in his opinion on the Commission proposal on EU-PNR the EDPS also raised the question of the data protection framework (first or third pillar)

([7]) See in particular Chapter 3 of the Report, 'Outstanding issues pertinent to transatlantic relations', point 1: 'Consistency in private entities obligations during data transfers'.

([8]) See on this issue the Opinion of the EDPS of 20 December 2007 on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, OJ C 110, 1.5.2008, p. 1. 'Traditionally, a clear separation has existed between law enforcement and private sector activities, where law enforcement tasks are performed by specifically dedicated authorities, in particular police forces, and private actors are solicited on a case by case basis to communicate personal data to these enforcement authorities. There is now a trend to impose cooperation for law enforcement purposes on private actors on a systematic basis'.

([9]) See the Opinion 10/2006 of the Article 29 Working Party of 22 November 2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128.

([10]) Opinion of 20 December 2007, op.cit.

([11]) See the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, mentioned in footnote 8, as presently discussed in Council.

applicable to the conditions of the cooperation between public and private actors: should the rules be based on the quality of the data controller (private sector) or on the purpose followed (law enforcement)? The dividing line between the first and third pillar is far from clear in situations where obligations are laid upon private actors to process personal data for purposes of law enforcement. It is in this context significant that Advocate General Bot in his recent opinion in the data retention case ([12]) proposes a dividing line for those situations but adds to this proposal: 'This dividing line is certainly not exempt from criticism and may appear artificial in some respects.' The EDPS also notes that the PNR-Judgement of the Court ([13]) does not fully answer the question of the applicable legal framework. For example, the fact that certain activities are not covered by Directive 95/46/EC does not automatically mean that those activities can be regulated under the third pillar. As a result, it possibly leaves a loophole as to applicable law and in any event results in legal uncertainty as to the legal guarantees available to data subjects.

23. In this perspective, the EDPS stresses that it must be ensured that a future instrument with general data protection principles cannot legitimise as such the transatlantic transfer of personal data between private and public parties. This transfer can only be included in a future instrument, provided that:

— the future instrument stipulates that the transfer is only allowed if it has proved to be absolutely necessary for a specific purpose, to be decided on a case by case basis,

— the transfer itself is surrounded by high data protection safeguards (as described in this Opinion).

Moreover, the EDPS notes the uncertainty about the applicable data protection framework and pleads therefore in any event not to include the transfer of personal data between private and public parties under the present state of EU law.

— Between public authorities:

24. The exact scope of the exchange of information is unclear. As a first step in the further work towards a common instrument, the envisaged scope of such an instrument should be clarified. Questions remain in particular whether:

— as far as databases situated in the EU are concerned, the instrument would aim at centralised databases (partially) managed by the EU such as the databases of Europol and Eurojust, or decentralised databases managed by Member States, or both,

— the scope of the instrument extends to interconnected networks, that is, whether guarantees foreseen will cover data that are exchanged between Member States or agencies, in the EU as well as in the US,

— the instrument would cover only the exchange between databases in the area of law enforcement (police, justice, possibly customs) or also other databases such as tax databases,

— the instrument would also relate to databases of national security agencies, or would allow for access by those agencies to law enforcement databases on the territory of the other contracting party (EU to US and vice versa),

— the instrument would cover case by case transfer of information, or permanent access to existing databases. This last hypothesis would certainly raise proportionality issues, as discussed further in Chapter V, under point 3.

Law enforcement purpose

25. The definition of the purpose of a possible agreement also leaves room for uncertainty. Law enforcement purposes are clearly indicated in the introduction as well as in the first principle annexed to the report, and will be further analysed in Chapter IV of this Opinion. The EDPS already notes that it appears from these statements that the exchange of data would focus on third pillar matters, but one could wonder whether this is only a first step towards a wider exchange of information. It seems clear that 'public security' purposes stated in the report include the fight against terrorism, organised crime and other crimes. However, is it also meant to allow for the exchange of data for other public interests such as possibly public health risks?

26. The EDPS recommends to restrict the purpose to precisely identified data processing, and to justify the policy choices leading to such definition of purpose.

([12]) Opinion of Advocate General Bot of 14 October 2008, Ireland v. European Parliament and Council (Case C-301/06), par. 108.

([13]) 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.

A global transatlantic security area

27. The broad scope of this report should be put in the perspective of the global transatlantic security area discussed by the so-called 'Future Group' ([14]). The report of this group, issued in June 2008, puts some focus on the external dimension of home affairs policy. It advocates that *'by 2014, the European Union should make up its mind with regard to the political objective to realise a Euro-Atlantic area of cooperation in the field of freedom, security and justice with the United States'*. Such cooperation would go beyond security in the strict sense and would at least include the subjects dealt with in the present Title IV of the EC Treaty such as immigration, visa and asylum and civil law cooperation. It must be questioned how far an agreement on basic data protection principles, such as those mentioned in the report of the HLCG, could and should be the basis for an exchange of information in such a wide area.

28. Normally, by 2014 the pillar structure will no longer exist and there will be one legal basis for data protection within the EU itself (under the Lisbon Treaty, Article 16 of the Treaty on the Functioning of the European Union). However, the fact that there is harmonisation at EU level with regard to *regulation* of data protection does not imply that any agreement with a third country could allow for the *transfer* of any personal data, whatever the purpose. Depending on the context and the conditions of processing, adapted data protection guarantees might be required for specific areas such as law enforcement. The EDPS recommends taking the consequences of these different perspectives into consideration in the preparation of a future agreement.

III.2. **Nature of the agreement**

The European institutional framework

29. For the short term in any case, it is essential to determine under which pillar the arrangement will be negotiated. This is needed especially because of the internal regulatory framework for data protection that will be affected by such an agreement. Will it be the first pillar-framework — basically Directive 95/46/EC with its specific regime for transfer of data to third countries — or will it be the third pillar framework with a less stringent regime for transfers to third countries ([15])?

30. While law enforcement purposes prevail, as already mentioned, the report of the HLCG nevertheless mentions collection of data from private actors, and the purposes can also be interpreted in a broad way that might go beyond pure security, including e.g. immigration and border control issues, but also possibly public health. In view of these uncertainties, it would be highly preferable to wait for the harmonisation of the pillars under EU law, as foreseen in the Lisbon Treaty, to establish clearly the legal basis for negotiations and the precise role of the European institutions, especially the European Parliament and the Commission.

Binding character of the instrument

31. It should be made clear whether the conclusions of the discussions will lead to a Memorandum of Understanding or another non-binding instrument, or whether it will consist of a binding international agreement.

32. The EDPS supports the preference in the report for a binding agreement. An official binding agreement is in the view of the EDPS an indispensable prerequisite to any data transfer outside the EU, irrespective of the purpose for which the data are being transferred. No transfer of data to a third country can take place without adequate conditions and safeguards included in a specific (and binding) legal framework. In other words, a Memorandum of Understanding or another non-binding instrument can be useful to give guidance for negotiations for further binding agreements, but can never replace the need for a binding agreement.

Direct effect

33. The provisions of the instrument should be binding equally on the US, and on the EU and its Member States.

34. It should furthermore be ensured that individuals are entitled to exercise their rights, and especially to obtain redress, on the basis of the agreed principles. According to the EDPS, this result can best be achieved if the substantive provisions of the instrument are formulated in such a way that they have direct effect vis-à-vis the residents of the European Union and can be invoked before a Court. The direct effect of the provisions of the international agreement, as well as the conditions of its transposition in internal European and national law to ensure the effectiveness of the measures, must therefore be made clear in the instrument.

Relation with other instruments

35. The extent to which the agreement stands alone, or has to be completed on a case by case basis by further agreements on specific exchanges of data is also a fundamental issue. It is indeed questionable whether a single agreement could cover in an adequate way, with one single set of

([14]) Report of the Informal High Level Advisory Group on the Future of the European Home Affairs Policy, 'Freedom, Security, Privacy — European Home Affairs in an open world', June 2008, available at register.consilium.europa.eu

([15]) See Articles 11 and 13 of the DPFD, mentioned in point 7 of this Opinion.

standards, the multiple specificities of data processing in the third pillar. It is even more doubtful that it could *allow*, without additional discussions and safeguards, for a blanket approval of any transfer of personal data whatever the purpose and the nature of the data concerned. Besides, agreements with third countries are not necessarily permanent, as they can be linked with specific threats, be subject to review, and be subject to sunset clauses. On the other hand, common minimum standards as recognised in a binding instrument could facilitate any further discussion on the transfer of personal data in relation to a specific database or processing operations.

36. The EDPS would therefore favour the development of a minimal set of data protection criteria to be complemented on a case by case basis by additional specific provisions, as mentioned in the HLCG report, rather than the alternative of a stand alone agreement. Those additional specific provisions are a precondition in order to allow for the transfer of data in a specific case. This would encourage a harmonised approach in terms of data protection.

Application to existing instruments

37. It should also be examined how a possible general agreement would combine with already existing agreements concluded between the EU and the US. It should be noted that these existing agreements do not have the same binding nature: to be mentioned in particular are the PNR agreement (the one presenting the more legal certainty), the Europol and Eurojust agreements, or the SWIFT exchange of letters ([16]). Would a new general framework supplement these existing instruments, or would they stay untouched, the new framework applying only to other future exchanges of personal data? In the view of the EDPS, legal consistency would require a harmonised set of rules, applying to and complementing both existing and future binding agreements on transfers of data.

38. The application of the general agreement to existing instruments would have as an advantage the strengthening of their binding character. This would be particularly welcome with regard to instruments which are not legally binding, like the SWIFT exchange of letters, as it would at least impose compliance with a set of general privacy principles.

IV. **GENERAL LEGAL EVALUATION**

39. This chapter will consider how the level of protection of a specific framework or instrument is to be assessed, including the question of the benchmarks to be used and the basic requirements necessary.

Adequate level of protection

40. According to the EDPS, it should be clear that one of the main results of a future instrument would be that transfer of personal data to the United States can only take place, in so far as the authorities in the United States guarantee an adequate level of protection (and vice versa).

41. The EDPS considers that only a real adequacy test would ensure sufficient guarantees as to the level of protection of personal data. He considers that a general framework agreement with a scope as broad as the one of the HLCG report would have difficulties to pass, as such, a real adequacy test. The adequacy of the general agreement could be acknowledged only if it is combined with an adequacy of specific agreements concluded on a case by case basis.

42. The appreciation of the level of protection provided by third countries is not an unusual exercise, in particular for the European Commission: adequacy is under the first pillar a requirement for transfer. It has been measured at several occasions under Article 25 of Directive 95/46/EC on the basis of specific criteria, and confirmed by decisions of the European Commission ([17]). Under the third pillar, such a system is not explicitly foreseen: measuring of the adequacy of protection is only prescribed in the specific situation of Articles 11 and 13 of the — not yet adopted — Data Protection Framework Decision ([18]) and is left to Member States.

43. In the present case, the scope of the exercise touches upon law enforcement purposes, and the discussions are conducted by the Commission under supervision of the Council. The context is different from the evaluation of the Safe Harbour principles or the adequacy of Canadian legislation, and has more connections with the recent PNR negotiations with the US and Australia which took place in a third pillar legal framework. However, the HLCG principles have also been mentioned in the context of the Visa Waiver Programme, which concerns border and immigration and hence first pillar issues.

44. The EDPS recommends that any adequacy finding under a future instrument should build on experiences in these

([16]) See footnote 2.

([17]) Commission decisions on the adequacy of the protection of personal data in third countries, including Argentina, Canada, Switzerland, the United States, Guernsey, the Isle of Man and Jersey, are available at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Restricted to the transfer to a third country or international body by a Member State of data received from a competent authority in another Member State.

different areas. He recommends the further development of the notion of 'adequacy' in the context of a future instrument, on the basis of similar criteria, as used in previous adequacy determinations.

Mutual recognition — reciprocity

45. A second element of the level of protection relates to the mutual recognition of the EU and US systems. The report of the HLCG mentions in this respect that the objective would be to 'obtain the recognition of the effectiveness of each other's privacy and data protection systems for the areas covered by these principles' ([19]), and to reach 'equivalent and reciprocal application of privacy and personal data protection law'.

46. To the EDPS it is obvious that mutual recognition (or reciprocity) is only possible if an adequate level of protection is guaranteed. In other words, the future instrument should harmonise a minimum level of protection (by way of an adequacy finding, taking into account the need for specific agreements on a case by case basis). Only under this precondition could reciprocity be acknowledged.

47. The first element to take into account is the reciprocity of substantive provisions on data protection. In the view of the EDPS, an agreement should deal with the concept of reciprocity of substantive provisions on data protection in a way ensuring on the one hand that data processing within the territory of the EU (and the US) fully respects the domestic laws on data protection, and on the other hand that processing outside the country of origin of data and falling within the scope of the agreement respects the principles of data protection as included in the agreement.

48. The second element is reciprocity of redress mechanisms. It should be ensured that European citizens have an adequate means of redress when data related to them are being processed in the United States (irrespective of the law that applies to that processing), but equally that the European Union and its Member States give equivalent rights to US-citizens.

49. The third element is reciprocity of access by law enforcement authorities to personal data. If any instrument allows the authorities of the United States access to data originating form the European Union, reciprocity would entail that the same access should be given to the authorities of the EU, in relation to data originating from the US. Reciprocity must not harm the effectiveness of the protection of the data subject. This is a precondition for allowing 'transatlantic' access by law enforcement authorities. This means, in concrete terms, that:

— Direct access by authorities of the United States to data within the territory of the EU (and vice versa) should not be allowed. Access should only be given on an indirect basis under a 'push'-system.

— This access should take place under the control of data protection authorities and the judicial authorities in the country where the data processing takes place.

— Access by authorities of the United States to data bases within the EU should respect the substantive provisions on data protection (see above) and ensure full redress to the data subject.

Precision of the instrument

50. The specification of the conditions of assessment (adequacy, equivalence, mutual recognition) is essential since it determines the content, in terms of preciseness, legal certainty and effectiveness of the protection. The content of a future instrument must be precise and accurate.

51. Besides, it should be clear that any specific agreement concluded in a further step will still need to include detailed and complete data protection safeguards in relation to the subject of the exchange of data envisaged. Only such a double level of concrete data protection principles would ensure the necessary 'close fit' between the general agreement and specific agreements, as already noted in points 35 and 36 of this Opinion.

Developing a model for other third countries

52. The extent to which an agreement with the US could be a model for other third countries deserves specific attention. The EDPS notes that besides the US, the above-mentioned report of the Future Group also indicates Russia as a strategic partner of the EU. As far as the principles are neutral and in compliance with fundamental EU safeguards, they could constitute a useful precedent. However, specificities linked e.g. to the legal framework of the recipient country or the purpose of the transfer would prevent the pure transposition of the agreement. Equally decisive will be the democratic situation of third countries: it should be made sure that the principles agreed on will be effectively guaranteed and implemented in the recipient country.

What benchmarks to assess the level of protection?

53. An implicit or explicit adequacy should anyway comply with the International and European legal framework and especially the commonly agreed data protection safeguards.

([19]) Chapter A. Binding international agreement, p. 8.

These are enshrined in the United Nations Guidelines, Convention 108 of the Council of Europe and its additional protocol, the OECD-Guidelines and the draft Data Protection Framework Decision, as well as, for first pillar aspects, Directive 95/46/EC ([20]). All these instruments contain similar principles which are more widely recognised as the core of personal data protection.

54. It is all the more important that the principles mentioned above are duly taken into account, considering the impact of a potential agreement such as the one foreseen by the HLCG report. An instrument addressing the whole *enforcement* sector of a third country would indeed be a situation without precedent. Existing adequacy decisions in the first pillar, and agreements concluded with third countries in the third pillar of the EU (Europol, Eurojust) have always been linked with a specific transfer of data, while here transfers with a much broader scope might be rendered possible, considering the broad purpose followed (fighting criminal offences, national and public security, border enforcement) and the unknown number of databases concerned.

Basic requirements

55. The conditions to be complied with in the context of the transfer of personal data to third countries have been developed in a working document of the Article 29 Working Party ([21]). Any agreement on minimum privacy principles should meet a test of compliance ensuring the effectiveness of the data protection safeguards.

— On substance: data protection principles should provide for a high level of protection, and meet standards in line with EU principles. The 12 principles included in the report of the HLCG will be further analysed in this perspective in Chapter V of this Opinion.

— On specificity: depending on the nature of the agreement, and especially if it constitutes an official international agreement, the rules and procedures should be detailed enough, in order to allow for an effective implementation.

— On oversight: to ensure compliance with the rules agreed on, specific mechanisms of control should be put in place, both internally (audits) and externally (reviews). These mechanisms must be equally available to both parties to the agreement. Oversight includes mechanisms to ensure compliance on the macro level such as joint review mechanisms, as well as compliance on the micro level, such as individual redress.

56. Besides these three basic requirements, particular attention should be paid to the specificities linked with the processing of personal data in a law enforcement context. This is indeed an area where fundamental rights can suffer some restrictions. Safeguards should therefore be adopted to compensate the restriction to individuals' rights, especially with regard to the following aspects, in view of the impact on the individual:

— Transparency: information and access to personal data might be limited in a law enforcement context, due for instance to the needs of discrete investigations. While within the EU additional mechanisms are traditionally put in place to compensate this limitation of fundamental rights (often involving independent data protection authorities), it must be ensured that similar compensation mechanisms will be available once the information is transferred to a third country.

— Redress: for the reasons mentioned above, individuals should benefit from alternative possibilities to have their rights defended, in particular via an independent supervisory authority and before a tribunal.

— Data retention: the justification for the period of retention of data might not be transparent. Measures must be taken so that this does not prevent effective exercise of rights by data subjects or by supervisory authorities.

([20]) — United Nations guidelines concerning computerised personal data files, adopted by the General Assembly on 14 December 1990, available at www.unhchr.ch/html/menu3/b/71.htm
— Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981, available at www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980, available at www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters available at http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— 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, OJ L 281, 23.11.1995, p. 31.

([21]) Working document of 24 July 1998 on Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive; WP12.

— Accountability of law enforcement authorities: in the absence of effective transparency, control mechanisms either by the individual or institutional stakeholders can by no means be comprehensive. It would still be crucial that such controls be firmly established, in view of the sensitivity of data and the coercive measures that can be taken against individuals on the basis of the processing of the data. Accountability is a decisive issue in respect of national control mechanisms of the recipient country, but also in respect of review possibilities by the country or region of origin of the data. Such review mechanisms are foreseen in specific agreements like the PNR agreement and the EDPS strongly recommends including them in the general instrument as well.

V. **ANALYSIS OF THE PRINCIPLES**

Introduction

57. This chapter analyses the 12 principles included in the document of the HLCG from the following perspective:

— These principles show that the US and the EU have some common views on the level of principles, as similarities can be noted with the principles of Convention 108.

— However, an agreement on the level of the principles is not enough. A legal instrument should be strong enough to ensure compliance.

— The EDPS regrets that the principles are not accompanied by an explanatory memorandum.

— It should be clear, before entering in the description of the principles, that both parties have the same understanding of the wording used, for instance with regard to the notion of personal information or individuals protected. Definitions in that sense would be welcome.

1. Purpose specification

58. The first principle listed in the Annex to the HLCG report indicates that personal information shall be processed for legitimate law enforcement purposes. As mentioned above, this refers for the European Union to the prevention, detection, investigation or prosecution of criminal offences. For the US however, the interpretation of law enforcement goes beyond criminal offences and includes 'border enforcement, public security and national security purposes'. The consequences of such discrepancies between EU and US stated purposes are not clear. While the report mentions that in practice the purposes may coincide to a large extent, it remains decisive to know precisely to what extent they do *not* coincide. In the law enforcement area, in view of the impact of measures taken on individuals, the purpose limitation principle must be strictly complied with and the purposes stated must be clear and circumscribed. Taking into account the reciprocity envisaged in the report, the approximation of these purposes seems also essential. In short, a clarification of the understanding of this principle is needed.

2. Integrity/data quality

59. The EDPS welcomes the provision requiring accurate, relevant, timely and complete personal information, as necessary for lawful processing. Such a principle is a basic condition to any efficient processing of data.

3. Necessity/proportionality

60. The principle makes a clear link between the information collected and the necessity of this information to accomplish a law enforcement purpose laid down by law. This requirement of a legislative basis is a positive element to ascertain the legitimacy of the processing. The EDPS notes nevertheless that, although this reinforces the legal certainty of the processing, the legal basis for such processing consists in a law of a third country. A law of a third country cannot in itself constitute a legitimate basis for a transfer of personal data ([22]). In the context of the HLCG report, it seems assumed that the legitimacy of the law of a third country, i.e. the United States, is acknowledged in principle. It should be kept in mind that, if such reasoning can find justification here, considering the United States are a democratic State, the same scheme would not be valid and could not be transposed to relations with any other third country.

61. Any transfer of personal data must be relevant, necessary and appropriate according to the Annex to the report of the HLCG. The EDPS stresses that to be proportionate, the processing must not be unduly intrusive, and the modalities of the processing must be balanced, taking into account the rights and interests of data subjects.

62. For this reason, access to information should happen on a case by case basis, depending on practical needs in the context of a specific investigation. Permanent access by third country law enforcement authorities to databases situated in the EU would be considered as disproportionate and insufficiently justified. The EDPS recalls that even in the context of existing agreements on the exchange of

([22]) See in particular Article 7(c) and (e) of Directive 95/46/EC. In its Opinion 6/2002 of 24 October 2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, the Article 29 Working Party stated that 'it does not seem acceptable that a unilateral decision taken by a third country for reasons of its own public interest should lead to the routine and wholesale transfer of data protected under the directive'.

data, e.g. in the case of the PNR agreement, the exchange of data is based on specific circumstances and is concluded for a limited period of time ([23]).

63. Following the same logic, the period of retention of data should be regulated: data should be kept only as long as they are necessary, considering the specific purpose followed. If they are no more relevant in relation to the purpose identified, they should be deleted. The EDPS strongly opposes the constitution of data warehouses where information about non-suspected individuals would be stored in view of possible further need.

4. Information security

64. Measures and procedures to guard data against misuse, alteration and other risks are developed in the principles, as well as a provision limiting access to authorised individuals. The EDPS considers this as satisfactory.

65. Additionally, the principle could be complemented by a provision mentioning that logs should be kept of those accessing the data. This would strengthen the effectiveness of the safeguards to limit access and prevent misuse of the data.

66. Besides, mutual information should be foreseen in case of security breach: recipients in the US as well as in the EU would be responsible for informing their counterparts in case data they received have been subject to unlawful disclosure. This will contribute to enhanced responsibility towards a secure processing of the data.

5. Special categories of personal information

67. The principle prohibiting the processing of sensitive data is in the view of the EDPS considerably weakened by the exception, allowing for any processing of sensitive data for which domestic law provides 'appropriate safeguards'. Precisely because of the sensitive character of data, any derogation to the prohibition principle must be adequately and precisely justified, with a list of purposes and circumstances under which an identified type of sensitive data can be processed, as well as with an indication of the quality of controllers entitled to process such types of data. Among the safeguards to be adopted, the EDPS considers that sensitive data should not constitute as such an element that could trigger an investigation. They could be available in specific circumstances but only as additional information with regard to a data subject already under investigation. These safeguards and conditions must be enumerated in a limitative way in the text of the principle.

6. Accountability

68. As developed in points 55-56 of this Opinion, accountability of public entities processing personal data must be ensured in an effective way, and assurances must be given in the agreement on the way this accountability will be ensured. This is all the more important considering the lack of transparency traditionally associated with the processing of personal data in a law enforcement context. In this view, mentioning — as it is the case now in the Annex — that public entities shall be accountable without giving any further explanation on the modalities and consequences of such accountability, is not a satisfactory guarantee. The EDPS recommends that such explanation is given in the text of the instrument.

7. Independent and effective oversight

69. The EDPS fully supports the inclusion of a provision providing for independent and effective supervision, by one or several public supervisory authorities. He considers that it should be made clear how independence is interpreted, notably from whom these authorities are independent and to whom they report. Criteria are needed in this respect, which should take into account institutional and functional independence, in relation to the executive and legislative bodies. The EDPS recalls that this is an essential element to ensure effective compliance with the principles agreed on. Intervention and enforcement powers of these authorities are also crucial in view of the question of the accountability of public entities processing personal data, as mentioned above. Their existence and competences should be made clearly visible to data subjects, in order to allow them to exercise their rights, especially if several authorities are competent depending on the context of the processing.

70. Furthermore, the EDPS recommends that a future agreement should also provide for cooperation mechanisms between the supervisory authorities.

8. Individual access and rectification

71. Specific guarantees are needed when it comes to access and rectification in a law enforcement context. In that sense, the EDPS welcomes the principle stating that individuals shall/should be provided with access to and the means to seek 'rectification and/or expungement of their personal information'. However, some uncertainties remain as to the definition of individuals (all data subjects should be protected and not only citizens of the country concerned), and conditions in which individuals might be able to object to the processing of their information. Precisions are needed on the 'appropriate cases' under

([23]) The Agreement will expire and cease to have effect seven years after the date of signature unless the parties mutually agree to replace it.

which an objection could be made, or could not be made. It should be clear for data subjects in what circumstances — depending e.g. on the type of authority, the type of investigation or other criteria — they will be able to exercise their rights.

72. Besides, if there is no direct possibility to object to a processing for justified reasons, an indirect verification should be available, through the independent authority responsible for the oversight of the processing.

9. Transparency and notice

73. The EDPS stresses once more the importance of effective transparency, in order to enable individuals to exercise their rights, and to contribute to the general accountability of public authorities processing personal data. He supports the principles as drafted, and insists in particular on the need for general *and* individual notice to the individual. This is reflected in the principle as drafted in point 9 of the Annex.

74. However, the report in its Chapter 2, A. B ('Agreed upon principles') mentions that in the US transparency may include 'individually or in combination, publication in the Federal Register, individual notice, and disclosure in court proceedings'. It must be clear that a publication in an official journal is not sufficient in itself to guarantee the appropriate information of the data subject. In addition to the need for individual notice, the EDPS recalls that information must be provided in a form and in a language easily understandable to the data subject.

10. Redress

75. To guarantee the effective exercise of their rights, individuals must be able to lodge a complaint before an independent data protection authority, as well as have a remedy before an independent and impartial tribunal. Both redress possibilities should be equally available.

76. Access to an independent data protection authority is necessary as it provides for a flexible and less costly assistance, in a context — law enforcement — that can be rather opaque to individuals. Data protection authorities can also provide assistance in exercising access rights on behalf on data subjects, where exceptions prevent the latter to gain direct access to their personal data.

77. Access to the judicial system is an additional and indispensable guarantee that the data subjects can seek redress before an authority belonging to a branch of the democratic system distinct from the public institutions which actually process their data. Such an effective remedy before a court has been considered by the European Court of Justice ([24]) as 'essential in order to secure for the individual effective protection for his right. (…) [It] reflects a general principle of community law which underlies the constitutional traditions common to the Member States and has been enshrined in Articles 6 and 13 of the European Convention for the protection of human rights and fundamental freedoms.' The existence of a judicial remedy is also explicitly foreseen in Article 47 of the Charter of Fundamental Rights of the European Union, and in Article 22 of Directive 95/46/EC, without prejudice to any administrative remedy.

11. Automated individual decisions

78. The EDPS welcomes the provision providing for appropriate safeguards in case of automated processing of personal information. He notes that a common understanding of what is considered a 'significant adverse action concerning the relevant interests of the individual' would clarify the conditions of application of this principle.

12. Onward transfers

79. The conditions put to onward transfers are unclear for some of them. In particular, where the onward transfer must comply with international arrangements and agreements between the sending and the receiving countries, it should be specified whether this refers to agreements between the two countries having initiated the first transfer, or the two countries involved in the onward transfer. According to the EDPS, agreements between the two countries having initiated the first transfer is in any event needed.

80. The EDPS also notes a very broad definition of the 'legitimate public interests' allowing for an onward transfer. The scope of public security remains unclear, and the extension of transfers in case of breach of ethics or regulated professions appears unjustified and excessive in a context of law enforcement.

VI. **CONCLUSION**

81. The EDPS welcomes the joint work of the EU and the US authorities in the area of law enforcement where data protection is crucial. He wants to insist nevertheless on the fact that the issue is complex, in particular with regard to its precise scope and nature, and that it therefore deserves careful and in depth analysis. The

([24]) Case 222/84 *Johnston* [1986] ECR 1651; Case 222/86 *Heylens* [1987] ECR 4097; Case C-97/91 *Borelli* [1992] ECR I-6313.

impact of a transatlantic instrument on data protection should be carefully considered in relation to the existing legal framework and the consequences on citizens.

82. The EDPS calls for more clarity and concrete provisions especially on the following aspects:

— clarification as to the nature of the instrument, which should be legally binding in order to provide sufficient legal certainty,

— a thorough adequacy finding, based on essential requirements addressing the substance, specificity and oversight aspects of the scheme. The EDPS considers that the adequacy of the general instrument could only be acknowledged if combined with adequate specific agreements on a case by case basis,

— a circumscribed scope of application, with a clear and common definition of law enforcement purposes at stake,

— precisions as to the modalities according to which private entities might be involved in data transfer schemes,

— compliance with the proportionality principle, implying exchange of data on a case by case basis where there is a concrete need,

— strong oversight mechanisms, and redress mechanisms available to data subjects, including administrative and judicial remedies,

— effective measures guaranteeing the exercise of their rights to all data subjects, irrespective of their nationality,

— involvement of independent data protection authorities, in relation especially to oversight and assistance to data subjects.

83. The EDPS insists on the fact that any haste in the elaboration of the principles should be avoided as it would only lead to unsatisfactory solutions, with effects opposite to those intended in terms of data protection. The best way forward at this point would therefore be the development of a roadmap towards a possible agreement at a later stage.

84. The EDPS also calls for more transparency with regard to the process of elaboration of the data protection principles. Only with the involvement of all stakeholders, including the European Parliament, could the instrument benefit from a democratic debate and gain the necessary support and recognition.

Done at Brussels, 11 November 2008.

Peter HUSTINX

European Data Protection Supervisor

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee towards a European e-Justice Strategy

(2009/C 128/02)

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 [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 30 May 2008, the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee 'Towards a European e-Justice Strategy' (hereinafter further the Communication) was adopted. In accordance with Article 41 of Regulation (EC) No 45/2001, the EDPS submits the present opinion.

2. The Communication aims to propose an e-Justice Strategy that intends to increase citizens' confidence in the European area of justice. E-Justice's primary objective should be to help justice to be administered more effectively throughout Europe, for the benefit of the citizens. The EU's action should enable citizens to access information without being hindered by the linguistic, cultural and legal barriers stemming from the multiplicity of systems. A draft action plan and timetable for the various projects are annexed to the Communication.

3. This opinion of the EDPS comments upon the Communication as far as it relates to the processing of personal data, the protection of privacy in the electronic communications sector and the free movement of data.

II. BACKGROUND AND CONTEXT

4. The JHA Council [3] identified several priorities for the development of e-Justice in June 2007:

   — setting up a European interface, the e-Justice portal;

   — creating the conditions for networking of several registers, such as criminal records, insolvency registers, commercial and business registers and land registers;

   — starting the preparation for the use of ICT for the European payment order procedure;

   — improving of the use of videoconferencing technology in cross-border proceedings, in particular concerning the taking of evidence;

   — devising support tools for translation and interpretation.

5. Work on e-Justice has steadily progressed since then. In the opinion of the Commission, work done in this framework must ensure that priority be given to operational projects and to decentralised structures, while providing for coordination at European level, drawing on existing legal instruments and employing IT tools to improve their effectiveness. The European Parliament has also expressed its support for the e-Justice project [4].

6. Both in the civil and in the criminal field, the use of modern information technologies has consistently been encouraged by the Commission. This led to instruments such as the European payment order. The Commission has been managing since 2003 the 'portal' of the European Judicial Network in civil and commercial matters, accessible to the citizens in 22 languages. The Commission has also designed and set up the European Judicial Atlas. These tools are precursory elements of a future European framework for e-Justice. In the criminal area, the Commission has worked on a tool aiming to permit the exchange of information extracted from criminal records of the Member States [5]. Not only the Commission but also Eurojust has developed secure communication systems with national authorities.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] Doc. 10393/07 JURINFO 21.
[4] See the draft report of the European Parliament, Committee on Legal Affairs.
[5] See, in particular, the ECRIS system, mentioned below.

7. E-Justice intends to offer many opportunities to make the European judicial area more concrete for citizens in coming years. In order to set up an overall strategy for this important issue the Commission adopted the present Communication on e-Justice. The Communication lays down objective criteria for identifying priorities, especially for future projects at European level, in order to achieve concrete results within a reasonable time.

8. The Commission staff working document, an accompanying document to the Communication with an executive summary of the Impact Assessment, gives also some background information ([6]). The Impact Assessment report has been prepared taking into account the reactions of the Member States, judicial authorities, legal professions, citizens and business. The EDPS has not been consulted. The Impact Assessment report gave preference to a policy option to address the problems that combines European dimension and national competence. The Communication has opted for this policy option. The strategy will focus on the use of videoconference, creation of an e-Justice portal, improvement of translation facilities by developing automatic online translation tools, improvement of communication between judicial authorities, increased interconnection between national registers and online tools for European procedures (e.g. European Payment Order).

9. The EDPS supports the focus on the abovementioned actions. In general he supports a comprehensive approach of e-Justice. He endorses the threefold need to improve access to justice, cooperation between European legal authorities and the effectiveness of the justice system itself. As a result of this approach several institutions and persons are affected:

— the Member States, who have the primary responsibility for providing effective and trustworthy justice systems;

— the European Commission, in its role of guardian of the treaties;

— the judicial authorities of Member States, which need more sophisticated tools to communicate, especially in cross-border cases;

— the legal professions, citizens and businesses, who all advocate better use of IT tools with a view to achieving more satisfactory responses to their 'justice' needs.

10. The Communication is closely linked to the proposal of a Council decision on the establishment of the European Criminal Records Information System (ECRIS). On 16 September 2008, the EDPS adopted an opinion on this proposal ([7]). He supported the proposal, provided that a number of considerations were taken into account. In particular, he pointed out that additional data protection guarantees should compensate the current lack of a comprehensive legal framework on data protection in the field of cooperation between police and judicial authorities. He therefore emphasised the need for effective coordination in the data protection supervision of the system, which involves authorities of the Member States and the Commission as provider of the common communication infrastructure.

11. Some recommendations of this opinion that are worth recalling are:

— a reference of high level of data protection should be made as a precondition for the implementing measures to be adopted;

— the responsibility of the Commission for the common infrastructure of the system, as well as the applicability of Regulation (EC) No 45/2001, should be clarified to better ensure legal certainty;

— the Commission should also be responsible for the interconnection software — and not Member States — in order to improve the effectiveness of the exchange and to allow better supervision of the system;

— the use of automatic translations should be clearly defined and circumscribed, so as to favour mutual understanding of criminal offences without affecting the quality of the information transmitted.

12. These recommendations are still illustrative for the context in which the current Communication will be analysed.

III. THE EXCHANGE OF INFORMATION FORESEEN IN THE COMMUNICATION

13. E-Justice has a very wide-ranging scope, including in general the use of ICT in the administration of justice within the European Union. This covers a number of issues like projects providing litigants with information in a more effective way. This includes online information on judicial systems, legislation and case law, electronic

([6]) Commission staff working document, accompanying document to the Communication of the Council, the European Parliament and the European Economic and Social Committee 'Towards a European strategy on e-Justice', Executive summary of the impact assessment, 30.5.2008, SEC(2008) 1944.

([7]) See the Opinion of the EDPS on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of framework Decision 2008/XX/JHA, available on the EDPS website (http://www.edps.europa.eu 'consultation' and then 'opinions', '2008').

communication systems linking litigants and the courts and the establishment of fully electronic procedures. It covers also European projects like the use of electronic tools to record hearings and projects involving information exchange or interconnection.

14. Even if the scope is very wide, the EDPS has noticed that there will be information on criminal proceedings and on civil and commercial judicial systems, but not on administrative judicial systems. And there will be a link to a Criminal and a Civil Atlas, but not to an Administrative Atlas, although it might be better to have access by citizens and enterprises to judicial administrative systems, i.e. administrative law and complaint procedures. Also a link to the Association of Councils of State should be provided for. These additions could be better for the citizens trying to find their way through the forest — which is often administrative law with all its tribunals — in order to become better informed on administrative judicial systems.

15. Therefore, the EDPS recommends including administrative procedures in e-Justice. As part of this new element, e-Justice projects should be initiated to enhance the visibility of data protection rules as well as national data protection authorities, in particular in relation to the kinds of data processed in the framework of e-Justice This would be in line with the so-called 'London initiative', which was launched by data protection authorities in November 2006 and is aimed at 'Communicating Data Protection and Making It More Effective'.

IV. THE NEW FRAMEWORK DECISION ON DATA PROTECTION IN THE FIELD OF POLICE AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

16. Further to the increasing exchange of personal data between judicial authorities envisaged by the Communication, the applicable data protection legal framework acquires even more importance. In this context, the EDPS notes that, three years after the initial Commission proposal, the Council of the European Union adopted on 27 November the framework decision on the protection of personal data in the field of police and judicial cooperation in criminal matters ([8]). This new piece of legislation will provide a general data protection legal framework for 'third pillar' matters, in addition to the 'first pillar' data protection provisions of Directive 95/46/EC.

17. The EDPS welcomes this legal instrument as a first considerable step forward for data protection in police and judicial cooperation. However, the level of data protection achieved in the final text is not fully satisfactory. In particular, the framework decision only covers police and judicial data exchanged between Member States, EU authorities and systems, and does not include domestic data. Furthermore, the adopted framework decision does not lay down the obligation to distinguish between different categories of data subjects, such as suspects, criminals, witnesses and victims, to ensure that their data are processed with more appropriate safeguards. It does not provide full consistency with Directive 95/46/EC, in particular with regard to limiting the purposes for which personal data may be further processed. Nor does it provide for an independent group of relevant national and EU data protection authorities, which could ensure both better coordination between data protection authorities as well as a substantive contribution to the uniform application of the Framework decision.

18. This would mean that, in a context in which many efforts are put to develop common systems of cross-border exchange of personal data, divergences still exist with regard to the rules according to which these data are processed and the citizens can exercise their rights in different EU countries.

19. Once again the EDPS recalls that ensuring a high level of data protection in police and judicial cooperation, as well as consistency with Directive 95/46/EC, represents a necessary complement to other measures introduced or envisaged to facilitate the cross-border exchange of personal data in law enforcement. This stems not only from the citizens' right to the respect of the fundamental right to the protection of personal data, but also from the need of law enforcement authorities to ensure the quality of exchanged data — as confirmed by the annex to the Communication with regard to interconnection of criminal records — trust between authorities in different countries, and ultimately the legal validity of the evidence collected in a cross-border context.

20. Therefore, the EDPS, encourages the EU institutions to take these elements specifically into account not only when implementing the measures envisaged in the Communication but also with a view to starting as soon as possible the reflections on further improvements of the legal framework for data protection in law enforcement.

V. E-JUSTICE PROJECTS

E-justice tools at European level

21. The EPDS acknowledges that exchanges of personal data are essential elements of the creation of an area of Freedom, Security and Justice. For that reason the EDPS supports the proposal to an e-Justice strategy, while highlighting the importance of data protection in this context. Indeed, respect for data protection is not only a legal obligation, but also a key element for success of the envisaged systems, e.g. ensuring quality of data exchanges. This is equally valid for the institutions and

([8]) Publication on the Official Journal is still pending.

bodies when they process personal data as when new policies are developed. Rules and principles should be applied and followed in practice and especially taken into account in the design and building phase of information systems. Privacy and data protection are in essence 'key success factors' for a prosperous and balanced information society. It therefore makes sense to invest in them and do it as early as possible.

22. In this context, the EDPS underlines that the Communication does not provide for a central European database. He welcomes the preference for decentralised architectures. The EDPS recalls that he issued an opinion on ECRIS ([9]) and on the Prüm Initiative ([10]). In his opinion on ECRIS, the EDPS expressed that a decentralised architecture avoids additional duplication of personal data in a central database. In his opinion on the Prüm Initiative, he advised to properly take into account the scale of the system when discussing the interconnection between databases. In particular specific formats for communication of data, such as online requests for criminal records, also taking into account the language differences, should be established, and the accuracy of the data exchanges should be constantly monitored. These elements should be taken into account also in the context of initiatives stemming from the e-Justice strategy.

23. The European Commission intends to contribute to the reinforcement and development of e-Justice tools at European level, in close coordination with the Member States and other partners. At the same time as supporting Member States' efforts, it intends to develop a number of computer tools on its own to increase the interoperability of systems, facilitate the public's access to justice and communication among judicial authorities and achieve substantial economies of scale at European level. As to interoperability of the software used by the Member States, not all Member States must necessarily use the same software — although this would be the most practical option — but the software must be fully interoperable.

24. The EDPS recommends that the interconnection and interoperability of systems should duly take into account the purpose limitation principle and be built around data protection standards (privacy by design). Any form of interaction between different systems should be thoroughly documented. Interoperability should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this access via another information system. The EDPS wants to stress again that interoperability should not by itself justify circumventing the purpose limitation principle ([11]).

25. Furthermore, another crucial point is ensuring that enhanced trans-border exchange of personal data is accompanied by enhanced supervision and cooperation by data protection authorities. The EDPS has already highlighted, in his opinion of 29 May 2006 on the framework decision on the exchange of criminal records ([12]), that the proposed Framework decision should not only address the cooperation between the central authorities but also the cooperation between the various competent data protection authorities. This need has become even more important since the negotiations on the recently adopted framework decision on the protection of personal data processed in the framework of police and judicial cooperation ([13]) led to the deletion of the provision establishing a working group reuniting EU data protection authorities and coordinating their activities with regard to the processing of data in the framework of police and judicial cooperation in criminal matters. Therefore, with a view to ensure effective supervision as well as good quality of the trans-border circulation of data extracted from criminal records, mechanisms of effective coordination between data protection authorities should be provided ([14]). These mechanisms should also take into account the supervisory competence of the EDPS with regard to the s-TESTA infrastructure ([15]). E-justice tools could support these mechanisms which could be developed in close cooperation with the data protection authorities.

26. In § 4.2.1, the Communication points out that it will be important for exchange of information extracted from criminal records to go beyond judicial cooperation so as to incorporate other objectives, e.g. access to certain posts. The EDPS stresses that any processing of personal data for purposes other than those for which they were collected should respect the specific conditions laid down by the applicable data protection legislation. In particular, processing of personal data for further purposes should

([9]) See footnote 4, paragraph 18.
([10]) OJ C 89, 10.4.2008, p. 4.
([11]) OJ C 91, 19.4.2006, p. 53. See also the EDPS Comments on the Communication of the Commission on interoperability of European databases, Brussels, 10.3.2006.
([12]) OJ C 91, 26.4.2007, p. 9.
([13]) See above, chapter IV.
([14]) See EDPS opinion of the on ECRIS, points 8 and 37-38.
([15]) On which, see below paragraph 27-28.

be allowed only if it is necessary to pursue interests listed in Community data protection legislation ([16]) and provided that they are laid down by legislative measures.

27. The Communication states, with regard to the interconnection of criminal records, that as part of preparations for the entry into force of the framework decision on the exchange of information extracted from criminal records, the Commission will launch two feasibility studies in order to organise the project as it develops and to extend the exchange of the information to cover third-country nationals convicted of criminal offences. In 2009, the Commission will provide the Member States with software designed to enable all criminal records to be exchanged within a short time frame. This reference system, combined with the use of s-TESTA to exchange information, will generate economies of scale because Member States will not have to do their own development work. It will also make it easier to run the project.

28. In this perspective, the EDPS welcomes the use of the s-TESTA infrastructure, which has proved to be a reliable system for the exchange of data, and recommends that the statistical elements relating to the envisaged data-exchange systems should be defined in detail and duly take into account the need to ensure data protection supervision. For example, statistical data might explicitly include elements such as the number of requests for access or rectification of personal data, the length and the completeness of the update process, the quality of persons having access to these data as well as the cases of security breaches. Furthermore, statistical data and the reports based on them should be made fully available to competent data protection authorities.

Automatic translation and the database of translators

29. The use of automatic translation is a useful instrument and is likely to favour mutual understanding between relevant actors in Member States. However, the use of automatic translation should not result in diminishing the quality of the information exchanged, especially when this information is used to take decisions having legal effects for concerned persons. The EDPS points out that it is important to clearly define and circumscribe the use of the automatic translation. The use of automatic translation for the transmission of information which has not been accurately pre-translated, such as additional comments or specifications added in individual cases, is likely to affect the quality of the information transmitted — and thus of the decisions taken on their basis — and should in principle be excluded ([17]). The EDPS suggests taking into account this recommendation in the measures stemming from the Communication.

30. The Communication wants to create a database of legal translators and interpreters so that there will be an improvement of the quality of legal translation and interpretation. The EDPS subscribes to this aim, but reminds that this database will be subject to the application of relevant data protection law. In particular, should the database contain evaluation data about the performance of translators, it might be subject to prior checking by competent data protection authorities.

Towards a European e-Justice action plan

31. In paragraph 5, the Communication points out that responsibilities must be clearly allocated among the Commission, the Member States and other actors involved in judicial cooperation. The Commission will assume a general role of coordination by encouraging the exchange of practices and will design, set up and coordinate the information on the e-Justice portal. Besides, the Commission will continue to work to interconnect criminal records and will continue to assume direct responsibility for the civil legal network and support the criminal legal network. The Member States will have to update the information on their judicial systems that appears on the e-Justice site. Other actors are the civil and criminal legal networks and Eurojust. They will develop the tools necessary for more effective judicial cooperation, in particular automated translation tools and the secure exchanging system, in close contact with the Commission. A draft action plan and timetable for the various projects are annexed to the Communication.

32. In this context, the EDPS underlines that in the ECRIS system on the one hand no central European database is established and no direct access to databases such as those containing criminal records of other Member States is foreseen, whilst on the other hand on the national level the responsibilities for correct information are centralised with the central authorities of the Member States. Within this mechanism, Member States are responsible for the operation of national databases and for the efficient performance of the exchanges. It is not clear whether they are responsible for the interconnection software or not. The Commission will provide the Member States with software designed to enable all criminal records to be exchanged within a short timeframe. This reference system will be combined with the use of s-TESTA to exchange information.

33. The EDPS understands that also in the context of analogous e-Justice initiatives similar systems might be implemented and the Commission will be responsible for the common infrastructure, although this is not specified in the

([16]) See in particular Article 13 of Directive 95/46/EC and Article 20 of Regulation (EC) No 45/2001.

([17]) See paragraph 39-40 of the EDPS opinion on ECRIS.

Communication. The EDPS suggests clarifying this responsibility in the measures stemming from the Communication, for reasons of legal certainty.

E-Justice projects

34. The annex lists a series of projects to be developed during the next five years. The first project, Development of e-Justice pages, is about the e-Justice portal. The action needs a feasibility study and development of the portal. Besides this, it needs an implementation of management methods and online information in all EU languages. The second and the third project are about the interconnection of criminal records. Project 2 is about interconnection of national criminal records. Project 3, envisages the creation of a European register of convicted third-country nationals, further to a feasibility study and the submission of a legislative proposal. The EDPS notes that the latter project is no longer mentioned in the Commission work programme, and wonders whether this reflects a change in the Commission's envisaged projects or just a postponement of this specific project.

35. The Communication also lists three projects in the area of electronic exchanges and three projects in the field of aid for translation. A pilot project will start on gradual compilation of comparative multilingual legal vocabulary. Other relevant projects relate to the creation of dynamic forms to accompany European legislative texts as well as fostering the use of videoconferencing by judicial authorities. Finally, as part of e-Justice forums, annual meetings will be held on e-Justice themes and training of legal professional in judicial cooperation will be developed. The EDPS suggests that such meetings and trainings pay sufficient attention to laws and practices on data protection.

36. The annex therefore envisages a broad range of European tools, with a view to facilitating exchange of information between actors in different Member States. Among these tools, an important role will be played by the e-Justice portal, for which the Commission will be mainly responsible.

37. A common characteristic of many of these tools will be that information, and personal data, will be exchanged and managed by different actors both at national and EU level, which are subjects to data protection obligations and supervisory authorities established on the basis of Directive 95/46/EC or Regulation (EC) No 45/2001. In this respect, as the EDPS has already made clear in his opinion on the Internal Market Information (IMI) system ([18]), it is essential to ensure that responsibilities with regard to compliance with data protection rules is ensured in an efficient and seamless way.

38. This requires basically on the one hand that responsibilities for processing of personal data within these systems are clearly defined and allocated; on the other hand, that appropriate coordination mechanisms — especially with regard to supervision — are laid down whenever necessary.

39. The use of new technologies is one of the cornerstones of the e-Justice initiatives: the interconnection of national registers, the development of electronic signature, secure networks, virtual exchange platforms and the enhanced use of videoconferencing will be essential elements of e-Justice initiatives in the course of the next years.

40. In this context, it is essential that data protection issues are taken into account at the earliest possible stage and are embedded into the architecture of the envisaged tools. In particular, both the architecture of the system and the implementation of adequate security measures are especially important. This 'privacy-by-design' approach would allow that the relevant e-Justice initiatives provide for effective management of personal data while ensuring compliance with data protection principles and security of data exchanges between different authorities.

41. Furthermore, the EDPS highlights that technology tools should be used not only to ensure the exchange of information, but also to enhance the rights of the persons concerned. In this perspective, the EDPS welcomes that the Communication refers to the possibility of citizens to request their criminal records online and in the language of their choice ([19]). With regard to this issue, the EDPS recalls that he welcomed, in his opinion on the Commission proposal on exchange of criminal records, the possibility for the person concerned to request information on his/her own criminal records to the central authority of a Member State, provided that the person concerned is or has been a resident or a national of the requested or requesting Member State. The idea of using as a 'one-stop-shop' the authority which is closer to the person concerned was also put forward by the EDPS in the area of coordination of social security systems. Therefore, the EDPS encourages the

([18]) OJ C 270, 25.10.2008, p. 1.
([19]) See p. 6 of the Communication.

Commission to go further on the same path, by fostering technology tools — and, in particular, online access — allowing citizens to be in better control of their personal data even when they move between different Member States.

VI. **CONCLUSIONS**

42. The EDPS supports the present proposal to establish e-Justice and recommends taking into account the observations made in this opinion, which includes:

— taking into account the recent framework decision on the protection of personal data in the field of police and judicial cooperation in criminal matters — including its shortcomings — not only when implementing the measures envisaged in the Communication, but also with a view to starting as soon as possible the reflections on further improvements of the legal framework for data protection in law enforcement;

— including administrative procedures in e-Justice. As part of this new element, e-Justice projects should be initiated to enhance the visibility of data protection rules as well as national data protection authorities, in particular in relation to the kinds of data processed in the framework of e-Justice projects;

— maintaining a preference for decentralised architectures;

— ensuring that the interconnection and interoperability of systems duly takes into account the purpose limitation principle;

— allocating clear responsibilities to all actors processing personal data within the envisaged systems and providing mechanisms of effective coordination between data protection authorities;

— ensuring that processing of personal data for purposes other than those for which they were collected should respect the specific conditions laid down by the applicable data protection legislation;

— clearly defining and circumscribing the use of automatic translations, so as to favour mutual understanding of criminal offences without affecting the quality of the information transmitted;

— clarifying Commission responsibility for common infrastructures, such as the s-TESTA;

— with regard to the use of new technologies, ensuring that data protection issues are taken into account at the earliest possible stage (privacy-by-design) as well as fostering technology tools allowing citizens to be in better control of their personal data even when they move between different Member States.

Done in Brussels, 19 December 2008.

Peter HUSTINX

European Data Protection Supervisor

Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare

(2009/C 128/03)

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,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 sent to the EDPS on 2 July 2008,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

The proposal for a directive on the application of patients' rights in cross-border healthcare

1. On 2 July 2008, the Commission adopted a proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare (hereinafter the proposal) [1]. The proposal was sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation (EC) No 45/2001.

2. The proposal aims at establishing a Community framework for the provision of cross-border healthcare within the EU, for those occasions where the care patients seek is provided in another Member State than in their home country. This is structured around three main areas:

   — the establishment of common principles in all EU health systems, defining clearly the Member States' responsibilities;

   — the development of a specific framework for cross-border healthcare, providing clarity on the patients' entitlements to have healthcare in another Member State;

   — the promotion of EU cooperation in healthcare, in areas like recognition of prescriptions issued in other countries, European reference networks, health technology assessment, data collection, quality and safety.

3. The objectives of this framework are twofold: to provide sufficient clarity about rights to be reimbursed for healthcare provided in other Member States, and ensure that the necessary requirements for high-quality, safe and efficient healthcare are ensured for cross-border care.

4. The implementation of a cross-border healthcare scheme requires the exchange of the relevant personal data relating to health (hereinafter health data) of the patients between the authorised organisations and healthcare professionals of the different Member States. These data are deemed as sensitive and fall under the stricter rules of data protection as laid down in Article 8 of Directive 95/46/EC on special categories of data.

EDPS consultation

5. The EDPS welcomes the fact that he is consulted on this issue and that reference to this consultation is made in the preamble of the proposal, in accordance with Article 28 of Regulation (EC) No 45/2001.

6. It is the first time that the EDPS has formally been consulted on a proposal for a Directive in the field of healthcare. In this Opinion, therefore, some of the remarks made are of a broader scope, addressing general issues of personal data protection in the healthcare sector, which could also be applicable for other relevant legal instruments (binding or not).

[1] COM(2008) 414 final. Please note that a complementary Communication on a Community framework on the application of patients' rights in cross-border healthcare (COM(2008) 415 final) was also adopted on the same date. However, since the Communication is only of rather general nature, the EDPS has chosen to focus on the proposed Directive.

7. Already at the outset, the EDPS would like to express his support to the initiatives of improving the conditions for cross-border healthcare. This proposal should in fact be seen in the context of the overall EC programme for improving the citizens' health in the information society. Other initiatives in this respect are the Commission's envisaged Directive and communication on human organs donation and transplantation ([1]), the recommendation on the interoperability of electronic health records ([2]), as well as the envisaged communication on telemedicine. ([3]) The EDPS is concerned, however, by the fact that all these related initiatives are not closely linked and/or interconnected in the area of privacy and data security, thus hampering the adoption of a uniform data protection approach in healthcare, especially with regard to the use of new ICT technologies. As an example, in the current proposal, although telemedicine is explicitly mentioned in recital 10 of the proposed directive, no reference to the relevant EC Communication's data protection dimension is made. Moreover, although electronic health records are a possible way of cross-border communication of health data, no link to the privacy issues addressed in the relevant Commission's recommendation is provided ([4]). This gives the impression that an overall healthcare privacy perspective is still not clearly defined and, in some cases, completely missing.

8. This is also evident in the current proposal, where the EDPS regrets to see that the data protection implications are not addressed in concrete terms. References to data protection can of course be found, but these are mainly of a general nature and do not adequately reflect the specific privacy-related needs and requirements of cross-border healthcare.

9. The EDPS wishes to emphasise that a uniform and sound data protection approach throughout the proposed healthcare instruments will not only ensure the citizens' fundamental right to protection of their data, but will also contribute to the further development of cross-border healthcare in the EU.

II. **DATA PROTECTION IN CROSS-BORDER HEALTHCARE**

General context

10. The most prominent aim of the European Community has been to establish an internal market, an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured. Enabling citizens to move to and reside more easily in other Member States than where they originate from obviously led to issues relating to healthcare. For that reason, back in the 1990s, the Court of Justice was confronted within the context of the internal market with questions on the possible reimbursement of medical expenses incurred in another Member State. The Court of Justice recognised that the freedom to provide services, as laid down in Article 49 of the EC Treaty, includes the freedom for persons to move to another Member State in order to receive medical treatment ([5]). As a consequence, patients who wanted to receive cross-border healthcare could no longer be treated differently from nationals in their country of origin who received the same medical treatment without crossing the border.

11. These Court judgments are at the heart of the current proposal. Since the Court's case law is based on individual cases, the current proposal intends to improve clarity to ensure a more general and effective application of the freedoms to receive and provide health services. But, as already mentioned, the proposal is also part of a more ambitious programme with the purpose of improving the citizens' health in the information society, where the EU sees great possibilities for enhancing cross-border healthcare through the use of information technology.

12. For obvious reasons, setting rules for cross-border healthcare is a delicate issue. It touches upon a sensitive area in which Member States have established diverging national systems, for instance with regard to the insurance and reimbursement of costs or the organisation of the healthcare infrastructure, including healthcare information networks and applications. Although the Community legislator in the current proposal only concentrates on *cross-border* healthcare, the rules will at least influence the way in which national healthcare systems are organised.

13. Improving the conditions for cross-border healthcare will be to the benefit of the citizens. However, it will at the same time embody certain risks for the citizens as well. Many practical problems which are inherent to cross-border cooperation between people from different countries speaking different languages have to be solved. Since a good health is of the utmost importance for every citizen, any risk of miscommunication and subsequent inaccuracy should be excluded. It goes without saying that enhancing cross-border healthcare in combination

([1]) Announced in the Commission's work programme.
([2]) Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282), OJ L 190, 18.7.2008, p. 37.
([3]) Announced in the Commission's work programme.
([4]) Illustrative in this respect is the fact that no reference to privacy or data protection is included in the Communication mentioned in footnote 1, which is intended to set out a Community framework on the application of patients' rights in cross-border healthcare.
([5]) See Case 158/96, *Kohll*, [1998] ECR I-1931, para 34. See amongst others also Case C-147/99, *Smits and Peerbooms* [2001] ECR I-5473 and Case C-385/99, *Müller-Fauré and Van Riet* [2003] ECR I-12403.

with the use of information technological developments, has great implications for the protection of personal data. A more efficient and therefore increasing exchange of health data, the increasing distance between persons and instances concerned, the different national laws implementing the data protection rules, lead to questions on data security and legal certainty.

Protection of health data

14. It must be emphasised that health data is considered a special category of data which deserves higher protection. As the European Court of Human Rights in the context of Article 8 of the European Convention of Human Rights recently stated: 'The protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention' ([1]). Before explaining the stricter rules for processing of health data which are laid down in Directive 95/46/EC, a few words will be devoted to the notion of 'health data'.

15. Directive 95/46/EC does not include an explicit definition of health data. Commonly, a wide interpretation is applied, often defining health data as 'personal data that have a clear and close link with the description of the health status of a person' ([2]). In this respect, health data normally includes medical data (e.g. doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs, etc.), as well as administrative and financial data relating to health (e.g. documents concerning hospital admissions, social security number, medical appointments scheduling, invoices for healthcare service provision, etc.). It should be noted that the term 'medical data' ([3]) is also sometimes used to refer to data relating to health, as well as the term 'healthcare data' ([4]). Throughout this Opinion the notion 'health data' will be used.

16. A useful definition of 'health data' is provided for by ISO 27799: 'any information which relates to the physical or mental health of an individual, or to the provision of health service to the individual, and which may include: (a) information about the registration of the individual for the provision of health services; (b) information about payments or eligibility for healthcare with respect to the individual; (c) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (d) any information about the individual collected in the course of the provision of health services to the individual; (e) information derived from the testing or examination of a body part or bodily substance; and (f) identification of a person (healthcare professional) as provider of healthcare to the individual'.

17. The EDPS is very much in favour of adopting a specific definition for the term 'health data' in the context of the current proposal, which could also be used in the future within other relevant EC legal texts (see Section III below).

18. Article 8 of Directive 95/46/EC sets out the rules on the processing of special categories of data. These rules are stricter than those for processing of other data as laid down in Article 7 of Directive 95/46/EC. This already shows where Article 8(1) explicitly states that the Member State *shall prohibit* the processing of, inter alia, data concerning health. In the subsequent paragraphs of the Article several exceptions to this prohibition are formulated, but these are narrower than the grounds for processing of normal data as set out in Article 7. For example, the prohibition does not apply if the data subject has given his or her *explicit* consent (Article 8(2)(a)), contrary to required *unambiguous* consent in Article 7 sub (a) of Directive 95/46/EC. Moreover, Member State law can determine that in certain cases even consent of the data subject cannot lift the prohibition. The third paragraph of Article 8 is solely dedicated to processing of data concerning health. According to this paragraph the prohibition of the first paragraph does not apply if the processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

19. Article 8 of Directive 95/46/EC lays much emphasis on the fact that the Member States should provide for suitable or adequate safeguards. Article 8(4) for instance allows Member States to lay down additional exceptions to the prohibition to process sensitive data for reasons of substantial public interest, but subject to the provision of suitable safeguards. This in general terms underlines the responsibility of Member States to attach special care to the processing of sensitive data, such as data concerning health.

Protection of health data in cross-border situations

Shared responsibilities between Member States

20. The Member States should be especially aware of the responsibility just mentioned once the issue of cross-border exchange of health data is at stake. As set out above, the cross-border exchange of health data increases the risk of inaccurate or illegitimate data processing.

([1]) See ECtHR 17 July 2008, *I v Finland* (appl. No 20511/03), para 38.
([2]) See Article 29 Working Party, working document on the processing of personal data relating to health in electronic health records (EHR), February 2007, WP 131, paragraph II.2. See also on the wide meaning of 'personal data': Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136.
([3]) Council of Europe, Recommendation No R(97)5 on the protection of medical data.
([4]) ISO 27799:2008 'Health informatics — Information security management in health using ISO/IEC 27002'.

Obviously this can have huge negative consequences for the data subject. Both the Member State of affiliation (where the patient is an insured person) and the Member State of treatment (where cross-border healthcare is actually provided) are involved in this process and therefore share this responsibility.

21. Security of health data is, in this context, an important issue. In the recent case cited above the European Court of Human Rights attached particular weight to the confidentiality of health data: 'Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general' ([1]).

22. The data protection rules, as laid down in Directive 95/46/EC, furthermore require that the Member State of affiliation should provide the patient with adequate, correct and up to date information about the transfer of his or her personal data to another Member State, together with ensuring the secure transfer of the data to this Member State. The Member State of treatment should also ensure secure receipt of this data and provide the appropriate level of protection when data is indeed processed, following its national data protection law.

23. The EDPS would like to make the Member States' shared responsibilities clear within the proposal, taking also into account the electronic data communication, especially in the context of new ICT applications, as this is discussed below.

Electronic health data communication

24. Improving cross-border exchange of health data is mainly established through the use of information technology. Although the exchange of data in a cross-border healthcare scheme may still be performed on paper (e.g. the patient moves to another Member State bringing all his/her relevant health data with him/her, like laboratory examinations, doctor referrals, etc.), it is clearly intended to use electronic means instead. Electronic communication of health data will be supported by healthcare information systems established (or to be established) in the Member States (in hospitals, clinics, etc.), as well as the use of new technologies, like the electronic healthcare record applications (operating possibly over the Internet), as well as other tools like patients and doctor health cards. Of course it is also possible that combined paper-based and electronic exchange forms are used, depending on the Member States healthcare systems.

25. E-health and telemedicine applications, which fall within the scope of the proposed Directive, will depend exclusively on the exchange of electronic health data (e.g. vital signs, images, etc.), usually in conjunction with other existing electronic healthcare information systems residing on the Member States of treatment and affiliation. This includes systems operating both at patient-to-doctor basis (e.g. remote monitoring and diagnosis), as well as at doctor-to-doctor basis (e.g. teleconsultation between healthcare professionals for expert advice on specific healthcare cases). Other more specific healthcare applications supporting the overall cross-border healthcare provision might also depend solely on electronic data exchange, e.g. electronic prescription (e-Prescription) or electronic referral (eReferral), which is already implemented at national level in some Member States ([2]).

Areas of concern in cross-border health data exchange

26. Taking into account the above mentioned considerations, together with the existing diversity of the Member States' health systems, as well as the growing development of e-health applications, the following two main areas of concern arise with regard to the protection of personal data in cross-border healthcare: (a) the different security levels which may be applied by the Member States for the protection of personal data (in terms of technical and organisational measures), and (b) privacy integration in e-health applications, especially in new developments. In addition, other aspects like secondary use of health data, especially in the area of statistics production, might also need special attention. These issues are further analysed in the remainder of this section.

Data security in the Member States

27. Despite the fact that Directives 95/46/EC and 2002/58/EC are uniformly applied in Europe, the interpretation and implementation of certain elements may differ between countries, especially in areas where the legal provisions are general and left up to the Member States. In this sense, main area of consideration is the security of the processing, i.e. the measures (technical and organisational) that the Member States take to safeguard the security of health data.

([1]) ECtHR 17 July 2008, *I v Finland* (appl. No 20511/03), para 38.

([2]) eHealth ERA Report, Towards the Establishment of a European eHealth Research Area, European Commission, Information Society and Media, March 2007, (http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf).

28. Although the strict protection of health data is a responsibility of all Member States, there is currently no commonly accepted definition of an 'appropriate' security level for healthcare within EU which could be applied in the case of cross-border healthcare. So, for example, a hospital in one Member State may be obliged by nationally imposed data protection regulations to adopt specific security measures (e.g. the definition of security policy and codes of conduct, specific rules for outsourcing and use of external contractors, auditing requirements, etc.) whereas in other Member States this might not be the case. This inconsistency may have impact on the cross-border data exchange, especially when in electronic form, since it cannot be guaranteed that data are secured (from a technical and organisational point of view) at the same level between different Member States.

29. There is, therefore, a need for further harmonisation in this field, in terms of defining a common set of security requirements for healthcare that should be commonly adopted by Member States' healthcare service providers. This need is definitely in line with the overall need for definition of common principles in the EU health systems, as set out in the proposal.

30. This should be done in a generic way, without imposing specific technical solutions to the Member States, but still setting a basis for mutual recognition and acceptance, e.g. in the fields of security policy definition, identification and authentication of patients and healthcare professionals, etc. Existing European and international standards (e.g. ISO and CEN) on healthcare and security, as well as well-accepted and legally based technical concepts (e.g. electronic signatures [1]) could be used as a road map in such an attempt.

31. The EDPS supports the idea of healthcare security harmonisation at EU level and is of the opinion that the Commission should undertake relevant initiatives, already in the framework of the current proposal (see Section III below).

Privacy in e-health applications

32. Privacy and security should be part of the design and implementation of any healthcare system, especially e-health applications as mentioned in this proposal (privacy-by-design). This undisputable requirement has already been supported in other relevant policy documents [2], both general, as well as healthcare specific [3].

33. In the framework of the e-health interoperability discussed within the proposal, the notion of 'privacy-by-design' should once more be stressed as a basis for all envisaged developments. This notion applies at several different layers: organisational, semantic, technical.

— At the organisational level, privacy should be considered in the definition of the necessary procedures for health data exchange between the Member States' healthcare organisations. This may have direct impact on the type of exchange and extend to which data are transferred (e.g. use of identification numbers instead of the patients' real names where this is possible).

— At the semantic level, privacy and security requirements should be incorporated within new standards and schemes, e.g. in the definition of the electronic prescription template as this is discussed within the proposal. This could build on existing technical standards in this field, e.g. standards on data confidentiality and digital signature, and address healthcare specific needs like role based authentication of qualified healthcare professionals.

— At the technical level, system architectures and user applications should adapt privacy enhancing technologies, implementing the aforementioned semantic definition.

34. The EDPS feels that the field of electronic prescriptions could serve as a start for the integration of privacy and security requirements at the very initial stage of development (see Section III below).

Other aspects

35. An additional aspect which could be considered in the framework of cross-border health data exchange is the secondary use of health data and in particular the use of data for statistical purposes, as already set out in the current proposal.

36. As mentioned earlier in point 18, Article 8(4) of Directive 95/46 foresees the possibility of secondary use of health data. However, this further processing should be done only for reasons of 'substantial public interest' and must be subject to 'suitable safeguards' laid down by national law or upon decision of the supervisory authority [4]. Moreover, in case of statistical data processing, as also mentioned in the EDPS opinion on the proposed regulation on

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13 , 19.1.2000, p. 12-20.

[2] The EDPS and EU Research and Technological Development, Policy Paper, EDPS, April 2008, (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf).

[3] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282), OJ L 190, 18.7.2008, p. 37.

[4] See also recital 34 of Directive 95/46. See on this point also the WP 29 Opinion on EHR mentioned above in footnote 8, at p. 16.

Community statistics on public health and health and safety at work [1], an additional risk arises from the different meaning the notions 'confidentiality' and 'data protection' might have in the application of data protection legislation on the one hand and legislation on statistics on the other hand.

37. The EDPS wishes to underline the above elements in the context of the current proposal. More explicit references to the data protection requirements regarding the subsequent use of health data should be included (see Section III below).

III. DETAILED ANALYSIS OF THE PROPOSAL

The proposal's provisions on data protection

38. The proposal includes a number of references to data protection and privacy in different parts of the document, more specifically:

— recital 3 states — among other things — that the Directive has to be implemented and applied with due respect for the rights to private life and protection of personal data;

— recital 11 refers to the fundamental right to privacy with respect to the processing of personal data, and confidentiality as two of the operating principles that are shared by health systems throughout the Community;

— recital 17 describes the right to the protection of personal data as fundamental right of the individuals that should be safeguarded, focusing especially on the individuals' right of access to health data — also in the context of cross-border healthcare — as this is established in Directive 95/46/EC;

— Article 3, which sets the relationship of the Directive with other Community provisions, refers in paragraph 1a to the Directives 95/46/EC and 2002/58/EC;

— Article 5 on the responsibilities of the Member State of treatment, sets in paragraph 1f the protection of the right to privacy as one of these responsibilities, in conformity with national measures implementing Directives 95/46/EC and 2002/58/EC;

— Article 6 on healthcare provided in another Member State, stresses in paragraph 5 the right of access for patients to their medical records when travelling to another Member State with the purpose of receiving healthcare there or seeking to receive healthcare provided in another Member State, again in conformity with national measures implementing Directives 95/46/EC and 2002/58/EC;

— Article 12 on the national contact point for cross-border healthcare, states in paragraph 2(a) that these contact points should be responsible — among other things — to provide and disseminate information to patients on the guarantees on the protection of personal data provided in another Member State;

— Article 16 on e-health, states that measures for achieving interoperability of information and communication technology systems should respect the fundamental right to the protection of personal data in accordance with the applicable law;

— lastly, in Article 18(1) it is mentioned — among other things — that the collection of data for statistical and monitoring purposes should be done in accordance with national and Community law on the protection of personal data.

39. The EDPS welcomes that data protection has been taken into account in the drafting of the proposal and that an attempt is made to show the overall need for privacy in the context of cross-border healthcare. However, the existing provisions of the proposal on data protection are either too general or refer to Member States' responsibilities in a rather selective and scattered way:

— in particular, recitals 3 and 11, together with Articles 3(1)(a), 16 and 18(1) are in fact addressing the general data protection legal framework (the last two in the context of e-health and statistics collection, but without setting specific privacy related requirements);

— as far as Member States' responsibilities are concerned, a general reference is made in Article 5(1)(f);

— recital 17 and Article 6(5) provide a more specific reference to the patients'right of access in the Member State of treatment;

— lastly, Article 12(2)(a) has a provision on the patients' right to information in the Member State of affiliation (through the operation of the national contact points).

In addition, as already mentioned in the Introduction of this Opinion, there is no link and/or reference to privacy aspects addressed in other EC legal instruments (binding or not binding) in the area of healthcare, especially with regard to the use of new ICT applications (like telemedicine or electronic health records).

[1] OJ C 295, 7.12.2007, p. 1.

40. In this way, although privacy is generally stated as a requirement of cross-border healthcare, the overall picture is still missing, both in terms of the Member States' obligations, as well as in terms of the particularities introduced through the cross-border nature of healthcare service provision (in contrast with national healthcare service provision). More specifically:

— Member States responsibilities are not presented in an integrated way, since some obligations (rights of access and information) are stressed — still in different parts of the proposal — whereas others are completely omitted, like security of processing;

— no reference is made to the concerns about Member States' inconsistencies on security measures and the need for health data security harmonisation at a European level, in the context of cross — border healthcare;

— no reference to privacy integration in e-health applications is made; this is also not adequately reflected in the e-Prescription case.

41. In addition, Article 18, which deals with data collection for statistical and monitoring purposes, raises some specific concerns. The first paragraph refers to 'statistical and *other additional data*'; it furthermore refers in plural to 'monitoring purposes' and subsequently lists the areas which are subject to these monitoring purposes, namely the provision of cross-border healthcare, the care provided, its providers and patients, the costs and outcomes. In this context, already quite unclear, a general reference to the data protection law is made, but no specific requirements relating to subsequent use of data concerning health as laid down in Article 8(4) of Directive 95/46/EC are set. Moreover, the second paragraph contains the unconditional obligation to transfer the large amount of data to the Commission at least on an annual basis. Since no explicit reference is made to an assessment of the necessity of this transfer, it seems that the Community legislator itself has already established the necessity of these transfers to the Commission.

The EDPS recommendations

42. In order to adequately address the aforementioned elements, the EDPS provides a number of recommendations, in terms of five basic steps for amendments, as described below.

Step 1 — Definition of health data

43. Article 4 defines the basic terms used within the proposal. The EDPS strongly recommends introducing in this article a definition of health data. A broad interpretation of health data should be applied, like the one described in Section II of this Opinion (points 14 and 15).

Step 2 — Introduction of a specific article on data protection

44. The EDPs also strongly recommends the introduction of a specific article on data protection within the proposal, which could set the overall privacy dimension in a clear and understandable way. This article should (a) describe the responsibilities of the Member States of affiliation and treatment, including — among other — the need for security of processing, and (b) identify the main areas for further development, i.e. security harmonisation and privacy integration in e-health. For these matters specific provisions can be made (within the proposed article), as presented in Steps 3 and 4 below.

Step 3 — Specific provision for security harmonisation

45. Following the amendment of Step 2, the EDPS recommends that the Commission adopts a mechanism for the definition of a commonly acceptable security level of the healthcare data at national level, taking into account existing technical standards in this field. This should be reflected in the proposal. A possible implementation could be through the use of comitology procedure, as this is already described in Article 19 and applies for other parts of the proposal. Moreover, additional instruments could be used for the production of relevant guidelines, including all concerned stakeholders, like the Article 29 Working Party and the EDPS.

Step 4 — Privacy integration in the e-Prescription template

46. Article 14 on the recognition of prescriptions issued in another Member State provides for the development of a Community prescription template, supporting interoperability of e-Prescriptions. This measure shall be adopted through a Comitology procedure, as this is defined in Article 19(2) of the proposal.

47. The EDPS recommends that the proposed e-Prescription template incorporates privacy and security, even at the very basic semantic definition of this template. This should be explicitly mentioned in Article 14(2)(a). Again the involvement of all relevant stakeholders is of major importance. In this respect, the EDPS wishes to be informed about and involved in further actions taken on this issue through the proposed Comitology procedure.

Step 5 — Subsequent use of health data for statistical and monitoring purposes

48. In order to prevent misunderstandings, the EDPS encourages clarifying the notion 'other additional data' in article 18(1). The Article should furthermore be amended in the sense that it refers more explicitly to the requirements for subsequent use of health data as laid down in Article 8(4) of Directive 95/46/EC. Moreover, the obligation to transmit all the data to the Commission, contained in the second paragraph, should be made subject to an assessment of the necessity of such transfers for legitimate purposes which are duly specified in advance.

IV. **CONCLUSIONS**

49. The EDPS would like to express support to the initiatives of improving the conditions for cross-border healthcare. He expresses concerns, however, about the fact that EC healthcare related initiatives are not always well co-ordinated with regard to ICT use, privacy and security, thus hampering the adoption of a universal data protection approach towards healthcare.

50. The EDPS welcomes that reference to privacy is made within the current proposal. However, a number of amendments are needed, as explained in Section III of this Opinion, in order to provide clear requirements, both for the Member States of treatment and affiliation, as well to properly address the data protection dimension of cross-border healthcare.

— A definition of health data should be included in Article 4, covering any personal data that can have a clear and close link with the description of the health status of a person. This should in principle include medical data, as well as administrative and financial data relating to health.

— The introduction of a specific article on data protection is strongly recommended. This article should set clearly the overall picture, describing the responsibilities of the Member States of affiliation and treatment and identifying the main areas for further development, i.e. security harmonisation and privacy integration, especially in e-health applications.

— It is recommended that the Commission adopts a mechanism in the framework of this proposal for the definition of a commonly acceptable security level of the healthcare data at national level, taking into account existing technical standards in this field. Additional and/or complementary initiatives, including all concerned stakeholders, the Article 29 Working Party and the EDPS, should also be encouraged.

— It is recommended that the notion of 'privacy-by-design' is incorporated in the proposed Community template for e-Prescription (also at semantic level). This should be explicitly mentioned in Article 14(2)(a). The EDPS wishes to be informed about and involved in further actions taken on this issue through the proposed comitology procedure.

— It is recommended to specify the language of Article 18 and to include a more explicit reference to the specific requirements relating to subsequent use of data concerning health as laid down in Article 8(4) of Directive 95/46/EC.

Done in Brussels, 2 December 2008.

Peter HUSTINX

European Data Protection Supervisor

Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

(2009/C 128/04)

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 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,

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

Background

1. On 13 November 2007, the European Commission adopted a Proposal amending, among others, the Directive on privacy and electronic communications, usually referred to as the ePrivacy Directive [1] (hereinafter 'Proposal' or 'Commission's Proposal'). On 10 April 2008, the EDPS adopted an Opinion on the Commission's Proposal where he provided recommendations to improve the Proposal in an attempt to help ensure that the proposed changes resulted in the best possible protection of the privacy and personal data of individuals ('EDPS First Opinion') [2].

2. The EDPS welcomed the Commission's proposed creation of a mandatory security breach notification system requiring companies to notify individuals when their personal data have been compromised. Furthermore, he also praised the new provision enabling legal persons (e.g. consumer associations and Internet service providers) to take action against spammers to further supplement existing tools to fight spam.

3. During the Parliamentary discussions that preceded the European Parliament's first reading, the EDPS provided further advice by issuing comments on selected issues that arose in the reports drafted by the European Parliament committees competent for reviewing the Universal Service [3] and ePrivacy Directives ('Comments') [4]. The Comments primarily addressed issues related to the processing of traffic data and the protection of intellectual property rights.

4. On 24 September 2008, the European Parliament ('EP') adopted a legislative resolution on the ePrivacy Directive ('first reading') [5]. The EDPS viewed positively several of the EP amendments that were adopted following the EDPS Opinion and Comments mentioned above. Among the important changes was the inclusion of information society service providers (i.e. companies operating on the Internet) under the scope of the obligation to notify security breaches. The EDPS also welcomed the amendment enabling legal and natural persons to file actions for infringement of any provision of

[1] The review of the ePrivacy Directive is part of a broader review process which aimed at the creation of an EU telecoms authority, the review of Directives 2002/21/EC, 2002/19/EC, 2002/20/EC, 2002/22/EC and 2002/58/EC, as well as the review of Regulation (EC) No 2006/2004 (hereinafter altogether 'review of the telecom package').

[2] Opinion of 10 April 2008 on the Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ C 181, 18.7.2008, p. 1.

[3] Directive 2002/22/EC on universal service and users' rights related to electronic communications networks (Universal Service Directive), OJ L 108, 24.4.2002, p. 51.

[4] EDPS Comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal Service) & Directive 2002/58/EC (ePrivacy) of 2 September 2008. Available at: www.edps.europa.eu

[5] European Parliament legislative resolution of 24 September 2008 on the proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007) 698 — C6-0420/2007 — 2007/ 248 (COD)).

the ePrivacy Directive (not only for violation of the spam provisions as initially proposed by the Commission's Proposal). The Parliament's first reading was followed by the Commission's adoption of an amended proposal on the ePrivacy Directive (hereinafter 'Amended Proposal') ([6]).

5. On 27 November 2008, the Council reached a political agreement on a review of rules on the telecoms package, including the ePrivacy Directive, which will become the Council's Common Position ('Common Position') ([7]). The Common Position will be notified to the EP under Article 251(2) of the Treaty establishing the European Community, which may entail the proposal of amendments by the EP.

Overall views on the Council Position

6. The Council modified essential elements of the text of the Proposal and did not accept many of the amendments adopted by the EP. Whereas the Common Position certainly contains positive elements, on the whole, the EDPS is concerned about its content, in particular because the Common Position does not incorporate some of the positive amendments proposed by the EP, the Amended Proposal or the opinions of the EDPS and of European Data Protection Authorities issued through the Article 29 Working Party ([8]).

7. On the contrary, in quite a few cases, provisions in the Amended Proposal and EP amendments, offering safeguards to the citizens, are deleted or substantially weakened. As a result, the level of protection afforded to individuals in the Common Position is substantially weakened. It is for these reasons that the EDPS now issues a Second Opinion, hoping that as the ePrivacy Directive makes its way through the legislative process, new amendments will be adopted that will restore the data protection safeguards.

8. This Second Opinion focuses on some essential concerns and does not repeat all the points made in the EDPS' First Opinion or the Comments, which all remain valid. In particular, this Opinion discusses the following items:

— the provisions on security breach notification,

— the scope of application of the ePrivacy Directive to private and publicly accessible private networks,

— the processing of traffic data for security purposes,

— the ability of legal persons to take action for infringements of the ePrivacy Directive.

9. In addressing the above issues, this Opinion analyses the Council's Common Position and compares it with the EP first reading and Commission's Amended Proposal. The Opinion includes recommendations aimed at streamlining the provisions of the ePrivacy Directive and ensuring that the Directive continues to adequately protect the privacy and personal data of individuals.

II. THE PROVISIONS ON SECURITY BREACH NOTIFICATION

10. The EDPS supports the adoption of a security breach notification scheme pursuant to which authorities and individuals will be notified when their personal data have been compromised ([9]). Notices of security breaches may help individuals take the necessary steps to mitigate any potential damage that results from the compromise. Furthermore, the obligation to send notices informing of security breaches will encourage companies to improve data security and enhance their accountability regarding the personal data for which they are responsible.

11. The Commission's Amended Proposal, the European Parliament's first reading and the Council's Common Position represent three different approaches to security breach notification currently under consideration. Each of the three approaches has positive aspects. However, the EDPS believes there is room for improvement in each of the approaches and advises to take into account the recommendations described below in considering the final steps towards adoption of a security breach scheme.

([6]) Amended proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation, Brussels, 6.11.2008, COM (2008) 723 final.

([7]) Available at the public website of the Council.

([8]) Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), available at the website of the Article 29 Working Party.

([9]) This Opinion uses the word 'compromised' to refer to any breach of personal data that occurred as a result of the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, transmitted, stored or otherwise processed.

12. In analysing the three security breach notification schemes, there are five critical points to consider: (i) the definition of security breach; (ii) the entities covered by the obligation to notify ('covered entities'); (iii) the standard that triggers the obligation to notify; (iv) the identification of the entity responsible for determining whether a security breach meets or fails to meet the standard; and (v) the recipients of the notice.

Overview of the Commission, Council and EP approaches

13. The European Parliament, Commission and Council have all adopted varying approaches for notification of security breaches. The EP's first reading modified the original security breach notification scheme set forth in the Commission's Proposal ([10]). Under the EP's approach, the obligation to notify applies not only to providers of publicly available electronic communications services but also to information society service providers ('PPECS' and 'ISSPs'). Furthermore, under this approach all breaches of personal data would have to be notified to the national regulatory authority or to the competent authorities (together 'authorities'). If authorities were to determine that the breach is *serious*, they would require the PPECs and ISSPs to notify the person affected without delay. In case of breaches that represent imminent and direct danger, PPECS and ISSPs would notify individuals before notifying the authorities and not await a regulatory determination. An exception to the obligation to notify consumers covers entities that can demonstrate to the authorities that '*appropriate technical protection measures have been applied*' rendering the data unintelligible to any person who is not authorised to access it.

14. Under the Council's approach, notification also has to be provided to both subscribers and authorities, but only in cases where the *covered entity* deems the breach to represent *a serious risk* to the subscriber's privacy (i.e. identity theft or fraud, physical harm, significant humiliation or damage of reputation).

15. The Commission's Amended Proposal maintains the EP's obligation to notify authorities of all breaches. However, in contrast to the EP's approach, the Amended Proposal includes an exception to the notification requirement with respect to individuals concerned where the PPEC demonstrates to the competent authority that (i) no harm (e.g., economic loss, social harm or identity theft) is '*reasonably likely*' to occur as a result of the breach or (ii) '*appropriate technological protection measures*' have been applied to the data concerned by the breach. Thus, the Commission's approach includes a harm-based analysis in connection with individual notifications.

([10]) In particular, EP Amendments 187, 124 to 127 as well as 27, 21 and 32 address this issue.

16. It is important to note that under the EP ([11]) and Commission approaches it is *the authorities* who are ultimately charged with determining whether the breach is serious or reasonably likely to cause harm. By contrast, under the Council's approach, the decision is left up to the *concerned entities*.

17. Both the Council and Commission's approaches apply only to PPECS, and not, as does the EP approach, to ISSPs.

The definition of security breach

18. The EDPS is pleased to see that the three legislative proposals contain the same definition of security breach notification, which is described as '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, transmitted, stored or otherwise processed [...]*' ([12]).

19. As further described below, this definition is welcome insofar as it is broad enough to encompass most of the relevant situations in which notification of security breaches might be warranted.

20. First, the definition includes instances when an *unauthorised access* of personal data by a third party has taken place, such as the hacking of a server containing personal data and retrieving such information.

21. Second, this definition would also include situations where there has been a loss or disclosure of personal data, while unauthorised access has yet to be demonstrated. This would include such situations as where the personal data may have been lost (e.g. CD-ROMs, USB drives, or other portable devices), or made publicly available by regular users (employee data file made inadvertently and temporarily available to a publicly accessible area through the Internet). Because there often will be no evidence demonstrating that such data may or may not, at some point in time, be accessed or used by unauthorised third parties, it seems appropriate to include these instances within the scope of the definition. Therefore, the EDPS recommends maintaining this definition. The EDPS also recommends including the definition of security breach in Article 2 of the ePrivacy Directive, as this would be more consistent with the overall structure of the Directive and provide more clarity.

([11]) Except in cases of imminent and direct danger in which case covered entities must notify consumers first.

([12]) Article 2(i) of the Common Position and Amended Proposal and Article 3.3 of the EP first reading.

Entities that should be covered by the obligation to notify

22. The obligation to notify under the EP approach applies to both PPECS and ISSPs. However, under the Council and Commission schemes, only PPECS such as telecommunication companies and providers of Internet access will be obliged to notify individuals where they suffer security breaches leading to the compromise of personal data. Other sectors of activity, for example, online banks, online retailers, online health providers and others are not bound by this obligation. For the reasons developed below, the EDPS believes that from a public policy perspective it is critical to ensure that information society services which include online businesses, online banks, online health providers etc. are also covered by the notification requirement.

23. First, the EDPS notes that although telecom companies are certainly targets of security breaches that warrant a notification obligation, the same is true for other types of companies/providers. Online retailers, online banks, online pharmacies are as likely to suffer security breaches as telecom companies, if not more so. Therefore, risk considerations do not weigh in favor of limiting the scope of a breach notification requirement to PPECS. The need for a broader approach is illustrated by other countries' experience. For example, in the United States almost all of the States (more than 40 at this juncture) have enacted laws on security breach notification which have a wider scope of application, encompassing not only PPECS but any entity holding the required personal data.

24. Second, while a breach of the types of personal data regularly processed by PPECS clearly may impact an individual's privacy, the same is true, if not more so, for the types of personal information processed by ISSPs. Certainly banks and other financial institutions may be in possession of highly confidential information (e.g. bank account details), the disclosure of which may enable use for identity theft purposes. Also, the disclosure of very sensitive health-related information by online health services may be particularly harmful to individuals. Therefore, the types of personal data that may be compromised also call for a wider application of the security breach notification that would, at a minimum, include ISSPs.

25. Some legal issues have been raised against widening the scope of application of this article, i.e. the entities covered by this requirement. In particular, the fact that the overall scope of the ePrivacy Directive concerns only PPECS has been put forward as an obstacle to applying the obligation to notify also to ISSPs.

26. In this context, the EDPS would like to remind that: (i) there is no legal obstacle whatsoever to include other actors than PPECS in the scope of certain provisions of the directive. The Community legislator has a full discretion in this respect; (ii) there are other precedents in the existing ePrivacy Directive of application to entities other than PPECS.

27. For example, Article 13 applies not only to PPECS but to any company that sends unsolicited communications, requiring prior opt-in consent to do so. Moreover, Article 5(3) of the ePrivacy Directive, which prohibits inter alia the storing of information such as cookies in users' terminal equipment, is binding not only upon PPECS, but also upon anyone who attempts to store information or gain access to information stored in the terminal equipment of individuals. Moreover, in the current legislative process, the Commission has even proposed expanding the application of Article 5(3) when similar technologies (cookies/spyware) are not only delivered through electronic communication systems but through any other possible method (distribution through downloads from the Internet or via external data storage media, such as CD-ROMs, USB sticks, flash drives, etc.). All these elements are welcome and should be kept, but also set relevant precedents for the present discussion on scope.

28. Moreover, in the current legislative process the Commission and EP and arguably the Council, have proposed a new Article 6.6(a), discussed below, that applies to entities other than PPECS.

29. Finally, taken into account the comprehensive positive elements derived from the obligation to notify security breaches, citizens are very likely to expect these benefits not only when their personal data has been compromised by PPECS but also by ISSPs. Citizens' expectations may not be met if, for example, they are not notified when an online bank has lost their bank account information.

30. In sum, the EDPS is convinced that the full benefits of security breach notification will be better accomplished only if the scope of covered entities includes both PPECS and ISSPs.

The standard triggering notification

31. Regarding the trigger for the notification, as further explained below, the EDPS is of the view that the Amended Proposal's standard '*reasonably likely to harm*' is the most appropriate of the three proposed standards. However, it is important to ensure that 'harm' is sufficiently wide to cover all relevant instances of negative effects on the privacy or other legitimate interests of individuals. Otherwise, it would be preferable to create a new standard pursuant to which notification would be mandatory '*if the breach is reasonably likely to cause adverse effects to individuals*'.

32. As outlined in the previous section, the conditions under which notification to individuals must be provided (referred to as 'the trigger' or 'standard') vary under the EP, Commission and Council approaches. Obviously, the volume of notices that individuals will receive will depend, in large part, on the trigger or standard set for notification.

33. Under the Council and Commission schemes, notification has to be provided if the breach represents a '*serious breach to the subscriber's privacy*' (Council) and if '*harm to consumer interest is reasonably likely as a result of the breach*' (Commission). Under the EP scheme, the trigger for the notification to individuals is '*seriousness of the breach*' (i.e. notification to individuals is required if the breach is deemed '*serious*'). Notification is not necessary below this threshold ([13]).

34. The EDPS understands that if personal data have been compromised, it may be argued that individuals to whom the data belong are entitled to know, in all circumstances, about this occurrence. However, it is only fair to ponder whether this is an appropriate solution in the light of other interests and considerations.

35. It has been suggested that an obligation to send notices whenever personal data has been compromised, in other words without any limitations, may lead to over-notification and 'notice fatigue', which could result in desensitization. As further described below, the EDPS is sensitive to this argument; yet, at the same time he wants to stress his concern about over-notification being a possible indicator of a widespread failure of information security practices.

36. As mentioned above, the EDPS sees the potential negative consequences of over-notification and would like to help ensure that the legal framework adopted for security breach notification does not produce this result. If individuals were to receive frequent breach notices even in those situations where there are no adverse effects, harm or distress, we may end up undermining one of the key goals of providing notice as individuals may, ironically, ignore notices in those instances where they may actually need to take steps to protect themselves. Striking the right balance in providing meaningful notice is thus important because, if individuals do not react to notices received, the effectiveness of notification schemes is highly reduced.

37. In order to adopt an appropriate standard that will not lead to over-notification, in addition to considering the trigger for notice, other factors, notably, the definition of security breach and the information covered by the obligation to notify, must be considered. In this regard, the EDPS notes that under the three proposed approaches, the volume of notifications may be high in the light of the broad definition of security breach discussed above. This concern for over-notification is further underscored by the fact that the definition of security breach covers all types of personal data. Although the EDPS considers this to be the correct approach (not limiting the types of personal data subject to notification), as opposed to other approaches such as US laws where the requirements are focused on the sensitivity of the information, it is nevertheless a factor to be taken into account.

38. In the light of the above, and taking into account the different variables considered altogether, the EDPS finds it appropriate to include a threshold or standard below which notification is not mandatory.

39. The standards proposed, i.e. the breach represents a '*serious risk to privacy*' or is '*reasonably likely to harm*' both seem to include, for example, social or reputational harm and economic loss. For example, these standards would address instances of exposure to identity theft through the release of non-public identifiers such as passport numbers, as well as the exposure of information about an individual's private life. The EDPS welcomes this approach. He is convinced that the benefits of security breach notification would not be fully achieved if the notification system covered only breaches leading to economic harm.

([13]) See footnote 11 regarding the exception to this rule.

40. Of the two proposed standards, the EDPS prefers the Commission's standard *'reasonably likely to cause harm'*, because it would provide a more appropriate level of protection to individuals. Breaches are far more likely to qualify for notification if they are *'reasonably likely to cause harm'* to individuals' privacy than if they are to present a *'serious risk'* of such harm. Thus, covering only breaches presenting a serious risk to individuals' privacy would considerably limit the number of breaches that must be notified. Covering only such breaches would give an inordinate amount of discretion to PPECS and ISSPs as to whether notification is required, insofar as it would be much easier for them to justify a conclusion that no *'serious risk'* of harm exists than that no harm is *'reasonably likely to occur'*. While over-notification is surely to be avoided, on balance the benefit of the doubt must be given to protecting individuals' privacy interests, and individuals should be protected at the very least when a breach is reasonably likely to cause them harm. Moreover, the term *'reasonably likely'* will be more effective in practice, both for covered entities and competent authorities, as it requires an objective evaluation of the case and its relevant context.

41. Furthermore, breaches of personal data may cause harm which is difficult to quantify and which may differ. Indeed, the disclosure of the same type of data, depending of the individual circumstances, may cause significant harm to one individual and less to another. A standard that would require the harm to be material, significant or serious would not be appropriate. For example, the Council's approach, which requires that the breach *seriously* affects someone's privacy, would provide inadequate protection to individuals insofar as such standard requires the effect on privacy to be 'serious'. This also gives scope for a subjective evaluation.

42. While as described above *'reasonably likely to harm'* seems to be a suitable standard for security breach notification, the EDPS nevertheless remains concerned that it may not include all of the situations where notification to individuals is warranted, i.e. all situations where negative effects for the privacy or other legitimate rights of individuals are reasonably likely. For this reason a standard could be considered that would require notification *'if the breach is reasonably likely to cause adverse effects to individuals'*.

43. This alternative standard has the additional benefit of consistency with EU data protection legislation. Indeed, the Data Protection Directive refers often to adverse affects upon the rights and freedoms of data subjects. For example, Article 18 and Recital 49 which deal with the obligation to register data processing operations with the data protection authorities authorise Member States to exempt this obligation in cases where the processing *'is unlikely adversely to affect the rights and freedoms of data subjects'*. A similar wording is used in Article 16.6 of the Common Position in order to enable legal persons to file actions against spammers.

44. Furthermore, taking the above into account, one would also expect covered entities and particularly authorities competent to enforce data protection legislation to be more familiar with the above standard and thus facilitate their assessment as to whether a given breach meets the requisite standard.

Entity to determine whether a security breach meets or fails to meet the standard

45. Under the EP approach (except in cases of imminent danger) and Commission's Amended Proposal it will be up to the Member States' authorities to determine whether a security breach meets or fails to meet the standard that triggers the duty to notify individuals concerned.

46. The EDPS believes that the involvement of an authority plays an important role in the determination of whether the standard is met insofar as it is, to some extent, a guarantee for the correct application of the law. Such a system may prevent companies from inappropriately assessing the breach as not harmful/serious and thus avoiding notification when, in fact, such notification is necessary.

47. On the other hand, the EDPS is concerned that a regime whereby authorities are required to carry out the assessment may be impractical and difficult to apply, or may in practice turn out to be counterproductive. It may thus even diminish the data protection safeguards for individuals.

48. Indeed, under such an approach, data protection authorities are likely to be inundated with notifications of security breaches and may face serious difficulties in making the necessary assessments. It is important to remember that in order to make an assessment of whether a breach meets the standard, authorities will have to be provided with sufficient inside information, often of complex technical nature, which they will have to process very quickly. Taking into account the difficulty of the assessment and the fact that some authorities have limited resources, the EDPS fears that it will be very difficult for authorities to comply with this obligation and might take resources away from other important priorities. Furthermore, such a system may put undue pressure upon authorities; indeed, if they decide that the breach is not serious and nevertheless individuals suffer damage, the authorities could potentially be held responsible.

49. The above difficulty is further underscored if one takes into account that time is a key factor in minimising the risks derived from security breaches. Unless the authorities are able to make the assessment within very short time-limits, the additional time required by authorities to make such assessments may increase the damages suffered by concerned individuals. Therefore, this additional step that is meant to provide more protection for individuals may ironically result in offering less protection than systems based on direct notification.

50. For the above reasons, the EDPS considers that it would be preferable to set up a system whereby it should be up to concerned entities to make the assessment whether the breach meets or fails to meet the standard, as provided in the Council's approach.

51. However, to avoid risks of possible abuse, for example of entities declining to notify under circumstances where notification clearly is called for, it is of utmost importance to include certain data protection safeguards described below.

52. First, the obligation applying to covered entities to make determinations whether they have to notify must of course be accompanied by another obligation requiring the mandatory notification to authorities of all breaches that meet the required standard. Concerned entities should in those cases be required to inform the authorities of the breach and the reasons of their determination regarding the notification and the content of any notification made.

53. Second, authorities must be given a real oversight role. In exercising this role, authorities must be allowed, but not obliged, to investigate the circumstances of the breach and require any remedial action that may be appropriate ([14]). This should include not only the notification of individuals (when this has not yet taken place) but also the ability to impose an obligation to undertake a course of action to prevent further breaches. Authorities should be granted effective powers and resources in this regard, and authorities must have the necessary leeway to decide when to react to a notification of security breach. In other words, this would enable authorities to be selective and engage in investigations of, for example, large, truly harmful security breaches, verifying and enforcing compliance with the requirements of the law.

54. In order to achieve the above, in addition to the powers recognised under the ePrivacy Directive such as Article 15a.3 and Data Protection Directive, the EDPS recommends inserting the following language: '*If the subscriber or individual concerned has not already been notified, the competent national authority, having considered the nature of the breach, may require the PPECS or ISSP to do so*'.

55. Furthermore, the EDPS recommends the EP and the Council to confirm the obligation proposed by the EP (Amendment 122, Article 4.1.a) for entities to conduct a risk assessment and identification on their systems and the personal data that they intend to process. Based on this obligation, entities shall draw a tailored and accurate definition of the security measures which will be applied in their cases and which should be at the disposal of the authorities. If a security breach occurs, this obligation will help covered entities — and eventually also the authorities in their oversight role — to determine whether the compromise of such information may cause adverse effects or harm to individuals.

56. Third, the obligation applying to covered entities to make determinations regarding whether they have to notify individuals must be accompanied by an obligation to maintain a detailed and comprehensive internal audit trail describing any breaches that have occurred and any notifications thereof as well as any measures undertaken to avoid future breaches. This internal audit trail must be at the authorities' disposal for their review and possible investigation. This will enable authorities to carry out their oversight role. This could be achieved by adopting language along the following lines: '*The PPECS and ISSPs shall keep and maintain comprehensive records detailing all security breaches occurred, relevant technical information related thereto and remedial action taken. Records shall also contain a reference to all notifications issued to subscribers or individuals concerned and to the competent national authorities, including their date and content. The records shall be produced to the competent national authority at its request.*'

57. Of course, in order to ensure consistency in the implementation of this standard as well as other relevant aspects of the security breach framework, such as the format and procedures for the notification, it would be appropriate for the Commission to adopt technical implementing measures, after consultation with the EDPS, the Article 29 Working Party and relevant stakeholders.

([14]) Article 15a.3 recognises this oversight powers by establishing that '*Member States shall ensure that competent national authorities and, where relevant, other national bodies have all investigative powers and resources necessary, including the possibility to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.*'

Recipients of the notification

58. As to recipients of the notices, the EDPS prefers the EP's and Commission's terminology over the Council's. Indeed, the EP has replaced the word 'subscribers' with the words 'users'. The Commission uses 'subscribers' and 'individual concerned'. Both the EP and the Commission language would include as recipients of the notices not only current subscribers but also former subscribers and third parties, such as users who interact with some covered entities without subscribing to them. The EDPS welcomes this approach and calls upon the EP and the Council to maintain it.

59. However, the EDPS notes a number of inconsistencies with respect to terminology in the EP first reading which should be fixed. For example, the word 'subscribers' has been replaced in most cases, but not all, with the words 'users', in other cases with the word 'consumers.' This should be harmonised.

III. SCOPE OF APPLICATION OF THE ePRIVACY DIRECTIVE: PUBLIC AND PRIVATE NETWORKS

60. Article 3.1 of the current ePrivacy Directive establishes the entities primarily concerned by the Directive, i.e. those which process data '*in connection with*' provision of public electronic communication services in public networks (referred above as 'PPECS') ([15]). Examples of PPECS include providing access to the Internet, transmission of information through electronic networks, mobile and telephone connections, etc.

61. The EP passed an Amendment 121 modifying Article 3 of the initial Commission's Proposal, pursuant to which the scope of application of the ePrivacy Directive was broadened to include '*the processing of personal data in connection with the provision of publicly available electronic communications services in public and private communications networks and publicly accessible private networks in the Community, [...]*' (Article 3.1 ePrivacy). Unfortunately, the Council and Commission have found it difficult to accept this amendment and therefore have not incorporated this approach into the Common Position and the Amended Proposal.

Application of the ePrivacy Directive to publicly accessible private networks

62. For the reasons explained below and to help foster consensus, the EDPS encourages keeping the essence of Amendment 121. In addition, the EDPS suggests including an amendment to help further clarify the types of services that would be covered by the broadened scope.

63. Private networks often are used to provide electronic communications services such as Internet access to an undefined number of people, which could potentially be large. This is the case, for example with Internet access in Internet cafes as well as at Wi-Fi spots available in hotels, restaurants, airports, trains and in other establishments open to the public where such services are often provided as a complement to other services (beverages, accommodation, etc.).

64. In all of the above examples, a communications service, e.g. Internet access, is made available to the public not through a public network, but rather through what may be considered a private one, i.e. a privately operated network. Furthermore, although in the above cases, the communications service is provided to the public, because the type of network used is private rather than public, the provision of these services *arguably* is not covered by the entire ePrivacy Directive or at least by some of its articles ([16]). As a result, the fundamental rights of individuals guaranteed by the ePrivacy Directive are not protected in these instances and an uneven legal situation is created for users accessing the same Internet access services through public telecommunications means *vis-à-vis* those who access them via private ones. This despite the fact that the risk to individuals' privacy and personal data in all of these cases exists to the same degree as it does when public networks are used to convey the service. In sum, there does not appear to be a *rationale* justifying the differential treatment under the Directive of communications services provided over a private network versus those provided over a public network.

65. Therefore, the EDPS would support an amendment, such as Amendment 121 of the EP, pursuant to which the ePrivacy Directive would also apply to the processing of personal data in connection with the provision of publicly available electronic communications services in *private* communications networks.

66. The EDPS recognises, however, that this language could lead to unforeseeable and possibly unintended consequences. Indeed, the mere reference to private networks

([15]) *'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks'.*

([16]) A *contrario,* it could be argued that because the communications service is provided to the public, even if the network is private, the provision of such services is covered by the existing legal framework, despite the fact that the network is private. In fact, for example, in France employers providing Internet access to their employees have been deemed to be equivalent to providers of Internet access that offer Internet access on a commercial basis. This interpretation is not widely accepted.

could be interpreted to cover situations that clearly are not intended to be covered by the Directive. For example, it could be asserted that a literal or strict interpretation of this language could bring owners of WiFi-equipped homes ([17]), which enable anyone in their range (usually the home) to connect, under the scope the Directive; even though this is not the intention of Amendment 121. In order to avoid this outcome, the EDPS suggests rephrasing Amendment 121 including under the scope of application of the ePrivacy Directive *'the processing of personal data in connection with the provision of publicly available electronic communications services in public or publicly accessible private communications networks in the Community, ...'*

67. This would help to clarify that only private networks that are publicly accessible would be covered under the ePrivacy Directive. By applying the provisions of the ePrivacy Directive *only* to *publicly accessible private networks* (and not to all private networks) a limit is set so that the Directive will cover only communication services provided in private networks that are intentionally made accessible to the public. This formulation will help further underscore that *availability* of the private network *to members of the public at large* is the key factor in determining whether the Directive would cover (in addition to the provision of a publicly available communications service). In other words, independently of whether the network is public or private, if the network is intentionally made available to the public in order to provide a public communications service, such as Internet access, even if such service is complementary to another one (e.g. hotel accommodation), this type of service/network would be covered by the ePrivacy Directive.

68. The EDPS notes that the approach supported above pursuant to which the provisions of the ePrivacy Directive are applied to *publicly accessible private networks* is consistent with the approaches adopted in several Member States, where the authorities have already deemed such types of services as well as services provided in purely private networks under the scope of application of the national provisions implementing the ePrivacy Directive ([18]).

69. To further legal certainty regarding the entities covered by the new scope, it may be useful to include an amendment in the ePrivacy Directive defining 'publicly accessible private networks' which could read as follows: *'publicly accessible private network means a privately operated network to which members of the public at large ordinarily have access on an unrestricted basis, whether or not by payment or in conjunction with other services or offerings, subject to acceptance of the applicable terms and conditions.'*

70. In practice, the above approach would mean that private networks in hotels and other establishments that provide access to the Internet to the public at large via a private network would be covered. Conversely, the provision of communications services in purely private networks where the service is restricted to a limited group of identifiable individuals would not be covered. Therefore, for example, virtual private networks and consumer homes equipped with Wi-Fi, would not be covered by the Directive. Services provided through purely corporate networks would not be covered either.

Private networks under the scope of application of the ePrivacy Directive

71. The exclusion of private networks *per* se as suggested above should be considered as an *interim* measure which should be subject of further debate. Indeed, given on the one side the privacy implications of excluding purely private networks as such and, on the other side, that it affects a large number of people who usually access the Internet through corporate networks, in the future, this may need to be reconsidered. For this reason, and in order to foster debate on this topic, the EDPS recommends including a recital in the ePrivacy Directive pursuant to which the Commission would carry out a public consultation on the application of the ePrivacy Directive to all private networks, with the input of the EDPS, data protection authorities and other relevant stakeholders. In addition, the recital could specify that as a result of the public consultation, the Commission should make any appropriate proposal to expand or limit the types of entities that should be covered by the ePrivacy Directive.

72. In addition to the above, the different articles of the ePrivacy Directive should be amended accordingly so that all the operational provisions explicitly refer to publicly available private networks in addition to public networks.

IV. PROCESSING OF TRAFFIC DATA FOR SECURITY PURPOSES

73. During the legislative process related to the review of the ePrivacy Directive, companies providing security services asserted that it was necessary to introduce into the ePrivacy Directive a provision legitimising the collection of traffic data to guarantee effective online security.

([17]) Typically wireless Local Area Networks (LANs).
([18]) See footnote 16.

74. As a result, the EP inserted Amendment 181, which created a new Article 6.6(a) that would explicitly authorise the processing of traffic data for security purposes: *'Without prejudice to compliance with the provisions other than Article 7 of the Directive 95/46/EC and Article 5 of this Directive, traffic data may be processed for the legitimate interest of the data controller for the purpose of implementing technical measures to ensure the network and information security, as defined by Article 4(c) of Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, of a public electronic communication service, a public or private electronic communications network, an information society service or related terminal and electronic communication equipment, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. Such processing must be restricted to that which is strictly necessary for the purposes of such security activity'*.

75. The Commission Amended Proposal accepted this amendment in principle, but removed a key clause designed to ensure that the other provisions of the Directive had to be respected in removing the clause that reads *'Without prejudice […] … of this Directive'*). The Council adopted a redrafted version, which went yet another step further in watering down the important protections and balancing of interests that were built into Amendment 181, in adopting language that reads as follows: *'Traffic data may be processed to the extent strictly necessary to ensure […] the network and information security, as defined by Article 4(c) of Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.'*

76. As further explained below, Article 6.6(a) is unnecessary and subject to risk of abuse, particularly if adopted in a form that does not include the important safeguards, clauses respecting other provisions of the Directive, and balancing of interests. Therefore, the EDPS recommends to reject this Article, or at a minimum, ensure that any such article on this issue includes the types of safeguards that were included in Amendment 181 as adopted by the EP.

Legal grounds to process traffic data applicable to electronic communications services and other data controllers under current data protection legislation

77. The extent to which providers of publicly available electronic communications services may legally process traffic data is regulated under Article 6 of the ePrivacy Directive, which restricts the processing of traffic data to a limited number of purposes such as billing, interconnection, and marketing. This processing can only take place subject to specified conditions, such as consent of individuals in the case of marketing. In addition, other data controllers such as information society service providers may process traffic data under Article 7 of the Data Protection Directive which establishes that data controllers may process personal data if they comply with at least one of a list of enumerated legal bases, also referred to as legal grounds.

78. An example of one such legal basis is Article 7(a) of the Data Protection Directive, which requires consent of the data subject. For example, if an online retailer wishes to process traffic data for the purposes of sending advertisement or marketing materials, he must obtain the consent of the individual. Another legal basis set forth in Article 7 may allow, in certain instances, the processing of traffic data for security purposes by, for example, security companies offering security services. This is based on Article 7(f) which establishes that data controllers may process personal data if doing so is *'necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed, except when such rights are overridden by the interest for fundamental rights and freedoms of the data subject...'* The Data Protection Directive does not specify instances in which processing of personal data would meet this requirement. Instead, determinations are made by data controllers, on a case-by-case basis, often with the agreement of national data protection authorities and other authorities.

79. The interplay between Article 7 of the Data Protection Directive and the proposed Article 6.6(a) of the ePrivacy Directive should be considered. The proposed Article 6.6(a) is a specification of the circumstances under which the requirements of Article 7(f) described above would be met. Indeed, by authorising the processing of traffic data to help ensure network and information security, Article 6.6(a) enables such processing for the purposes of the legitimate interest pursued by the data controller.

80. As further explained below, the EDPS believes that the proposed Article 6.6(a) is neither necessary nor useful. Indeed, from a legal point of view, in principle, it is unnecessary to establish whether a particular type of data processing activity, in this case the processing of traffic data for security purposes, meets or fails to meet the requirements of Article 7(f) of the Data Protection Directive, in which case, consent of the individual may be necessary *ex* Article 7(a). As noted above, this assessment is usually made by data controllers, i.e. companies, at implementation level, in consultation with data protection authorities, and where necessary, by the courts. Generally speaking, the EDPS believes that, in specific cases, the legitimate processing of traffic data for security purposes, carried out without jeopardising fundamental rights and freedoms of individuals, is likely

to meet the requirements of Article 7(f) of the Data Protection Directive and can therefore be carried out. Moreover, there is no other precedent in the DP and ePrivacy Directives for singling out or providing special treatment for certain types of data processing activities that would satisfy the requirements of Article 7(f), and there has been no demonstrated need for such an exception. By contrast, as noted above, it appears that under many circumstances, this type of activity would fit comfortably within the current text. Therefore, a legal provision confirming this assessment is in principle unnecessary.

The EP, Council, and Commission versions of Article 6.6(a)

81. As explained above, although unnecessary, it is important to highlight that Amendment 181 as adopted by the EP was nevertheless drafted, to some extent, taking into account privacy and data protection principles embodied in data protection legislation. The EP Amendment 181 could further address the data protection and privacy interest, for example, by inserting the words 'in specific cases' in order to ensure the selective application of this article or by including an specific conservation period.

82. Amendment 181 contains some positive elements. It confirms that the processing should comply with any other data protection principle applicable to the processing of personal data ('*Without prejudice … to compliance with the provisions […] of the Directive 95/46/EC and […] of this Directive*'). Furthermore, although Amendment 181 permits the processing of traffic data for security purposes, it strikes a balance between the interests of the entity that processes traffic data and those of the individuals whose data is processed so that such data processing can take place only if the interests for the fundamental rights and freedoms of individuals are not overridden by those of the entity processing the data ('*except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject*'). This requirement is essential insofar as it may permit the processing of traffic data for specific cases; however, it would not enable an entity to process traffic data in bulk.

83. The Council's redrafted version of the amendment contains elements to be praised, such as retaining the term '*strictly necessary*' which underscores the limited scope of application of this Article. However, the Council version eliminates the data protection and privacy safeguards referred to above. While in principle general data protection provisions apply, irrespective if specific reference is made in every case, Council's version of Article 6.6(a) may nevertheless be interpreted as giving full discretionary powers to process traffic data without being subject to any data protection and privacy safeguards that apply whenever traffic data is processed. Therefore, it might be argued that traffic data may be collected, stored, and further used without having to comply with data protection principles and specific obligations that otherwise apply to responsible parties, such as the quality principle or the obligation of fair and lawful processing and to keep the data confidential and secure. Furthermore, because no reference is made to applicable data protection principles that impose time limits for storage of the information or to specific time limits within the article, the Council version may be interpreted as enabling the collection and processing of traffic data for security purposes for an unspecified period of time.

84. In addition, the Council has weakened the privacy protections in certain parts of the text by potentially broadening the language. For example, the reference to the '*legitimate interest of the data controller*' has been removed, raising doubts regarding the types of entities that would be able to avail themselves of this exception. It is of utmost importance to avoid opening the door to any user or legal entity to benefit from this amendment.

85. The recent experiences in the EP and Council demonstrate that it is difficult to define by law the extent and conditions under which the processing of data for security purposes can be lawfully executed. Any existing or future article is unlikely to remove the obvious risks of an overly broad application of the exception for reasons other than purely security related or by entities that should not be able to benefit from the exception. This is not to say that such processing may not take place in any event. However, whether and to what extent it could be carried out, may be better assessed at implementation level. Entities wishing to engage in such processing should discuss the scope and conditions with the data protection authorities and, possibly, with the Article 29 Working Party. Alternatively, the ePrivacy Directive could include an article allowing the processing of traffic data for security purposes, subject to explicit authorisation by data protection authorities.

86. Taking into account on the one hand the risks that Article 6.6(a) poses to the fundamental right to data protection and privacy of individuals, and on the other hand the fact that, as explained in this Opinion, from a legal point of view, this Article is unnecessary, the EDPS has come to the conclusion that the best outcome would be for the proposed Article 6.6(a) to be deleted altogether.

87. If any text along the lines of any current version of Article 6.6(a) is adopted, against the recommendation of the EDPS, it should in any event incorporate the data protection safeguards discussed above. It should also be properly integrated into the existing structure of Article 6, preferably as a new paragraph 2a.

V. THE ABILITY OF LEGAL PERSONS TO TAKE ACTION FOR INFRINGEMENTS OF THE ePRIVACY DIRECTIVE

88. The EP passed Amendment 133 giving the possibility for Internet access providers and other legal entities such as consumer associations to bring legal action against infringements of any of the provisions of the ePrivacy Directive ([19]). Unfortunately, neither the Commission nor the Council has accepted it. The EDPS considers this amendment as very positive and recommends maintaining it.

89. To understand the importance of this amendment one needs to realize that in the area of privacy and data protection the damage inflicted upon a person individually considered, is usually not sufficient in itself for him/her to initiate legal action before a court. Individuals normally do not go to court on their own because they were spammed or because their name was wrongly included in a directory. This amendment would permit consumer associations and trade unions representing the interest of consumers at a collective level to take legal action on their behalf before courts. A greater diversity of enforcement mechanisms is also likely to encourage a better level of compliance and therefore in the interest of an effective application of the provisions of the ePrivacy Directive.

90. There are legal precedents in some Member States' legal frameworks which already foresee the possibility of collective redress in order to allow consumers or interests groups to claim for compensation from the party who caused damage.

91. Moreover, some Member States' Competition laws ([20]) entitle consumers, interest groups (in addition to the *affected competitor*) to file a lawsuit against the breaching entity. The *ratio* behind this approach is that companies acting in breach of competition laws are likely to profit since consumers suffering only marginal damages are as a general rule reluctant to file a lawsuit. This rationale can be applied *mutantis mutandi* in the field of data protection and privacy.

92. More important, as mentioned above, entitling legal entities such as consumer associations and PPECS to file lawsuits fosters the position of consumers and it promotes overall compliance with data protection legislation. If breaching companies are facing a higher risk to be sued, they are likely to invest more in complying with data protection legislation, which in the long run increases the level of privacy and consumer protection. For all of these reasons, the EDPS calls upon the EP and the Council to adopt a provision enabling legal entities to bring legal action against infringements of any of the provisions of the ePrivacy Directive.

([19]) Article 13.6 of the EP first reading.
([20]) See, for example, 8 UWG — German law on Unfair Competition.

VI. CONCLUSION

93. The Council's Common Position, EP first reading and Commission's Amended Proposal contain, to varying degrees, positive elements that would serve to strengthen the protection of individuals' privacy and personal data.

94. However, the EDPS believes that there is room for improvement, particularly with respect to the Council's Common Position which, unfortunately, has not maintained some of the EP amendments intended to help ensure the adequate protection of individuals' privacy and personal data. The EDPS urges the EP and the Council to restore the privacy safeguards embedded in the EP first reading.

95. In addition, the EDPS believes that it would be appropriate to streamline some of the provisions of the Directive. This is particularly true in the case of the security breach provisions, as the EDPS believes that the full benefits of breach notification will be best realized if the legal framework is set right from the outset. Finally, the EDPS considers that it would be appropriate to improve and clarify the formulation of some of the provisions of the Directive.

96. In the light of the above, the EDPS urges the EP and the Council to increase efforts to improve and clarify some of the provisions of the ePrivacy Directive, while at the same time, reinstating the amendments adopted by the EP first reading aimed at providing an appropriate level of privacy and data protection. To this end, the points 97, 98, 99 and 100 below summarise the issues at stake and put forward some recommendations and drafting proposals. The EDPS calls upon all parties involved to take them into account as the ePrivacy Directive makes its way towards final adoption.

Security Breach

97. The European Parliament, Commission and Council have all adopted varying approaches for notification of security breaches. Differences between the three models exist regarding, inter alia, the entities covered by the obligation, standard or trigger for the notification, data subjects entitled to be notified, etc. There is a need for the EP and Council to do its utmost to come up with a solid legal framework for security breach. To this end, the EP and Council should:

— *Maintain* the definition of security breach in the EP, Council and Commission texts as it is broad enough to encompass most of the relevant situations in which notification of security breaches might be warranted.

— With respect to the scope of the entities to be covered by the proposed notification requirement, *include* providers of information society services. Online retailers, online banks, online pharmacies are as likely to suffer security breaches as telecom companies, if not more so. Citizens will expect to be notified not only when Internet access providers suffer security breaches but particularly when this happens to their online banks and online pharmacies.

— Regarding the trigger for the notification, the Amended Proposal's standard '*reasonably likely to harm*' is an appropriate standard which provides for the functionality of the scheme. However, it is important to ensure that 'harm' is sufficiently wide to cover all relevant instances of negative effects on the privacy or other legitimate interests of individuals. Otherwise, it would be preferable to create a new standard pursuant to which notification would be mandatory '*if the breach is reasonably likely to cause adverse effects to individuals*'. The Council's approach, which requires that the breach *seriously* affects someone's privacy, would provide inadequate protection to individuals insofar as such standard requires the effect on privacy to be 'serious'. This also gives scope for a subjective evaluation.

— While the involvement of an authority to determine whether a concerned entity must notify individuals certainly has positive effects, it may be impractical and difficult to apply, and might also take resources away from other important priorities. If authorities cannot react extremely quickly, the EDPS fears that such a system may even diminish the protection for individuals and put undue pressure upon authorities. Thus, on the whole, the EDPS advises to *setting up* a system where it is up to concerned entities to make the assessment as to whether they must notify.

— In order to enable authorities to exercise oversight over the assessments made by covered entities regarding whether to notify, *implement* the following safeguards:

  — *Ensure* that such entities are obliged to notify authorities of all breaches that meet the requisite standard.

  — *Provide* authorities with an oversight role that enables them to be selective in order to be effective. To achieve the above, insert the following language: 'If the subscriber or individual concerned has not already been notified, the competent national authority, having considered the nature of the breach, may require the PPECS or ISSP to do so'.

  — *Adopt* a new provision requiring entities to maintain a detailed and comprehensive internal audit trail. This could be achieved by adopting the following language: 'The PPECS and ISSPs shall keep and maintain comprehensive records detailing all security breaches that occurred, relevant technical information related thereto, and remedial action taken. Records shall also contain a reference to all notifications issued to subscribers or individuals concerned and to the competent national authorities, including their date and content. The records shall be produced to the competent national authority at its request.'

— In order to ensure consistency in the implementation of the security breach framework, *provide* the Commission with the ability to adopt technical implementing measures, following prior consultation with the EDPS, the Article 29 Working Party and other relevant stakeholders.

— Concerning the individuals to be notified, *use* the Commission or EP's terminology 'individuals concerned' or 'affected users' as it includes all the individuals whose personal data has been compromised.

Publicly Accessible Private Networks

98. Communications services are often made available to the public not through public networks, but through privately operated networks (e.g. Wi-Fi spots available in hotels, airports), which are arguably not covered by the Directive. The EP adopted Amendment 121 (Article 3) broadening the scope of application of the Directive to include public and private communications networks, as well as publicly accessible private networks. In this regard, the EP and Council should:

— *Keep* the essence of Amendment 121, but rephrase it to include under the scope of the ePrivacy Directive only '*the processing of personal data in connection with the provision of publicly available electronic communications services in public or publicly accessible private communications networks in the Community*'. Purely privately operated networks (as opposed to publicly accessible private networks) would not be explicitly covered.

— *Amend* accordingly all the operational provisions to explicitly refer to publicly accessible private networks in addition to public networks.

— *Include* an amendment defining '*publicly accessible private network means a privately operated network to which members of the public at large ordinarily have access on an unrestricted basis, whether or not by payment or in conjunction with other services or offerings, subject to acceptance of the applicable terms and conditions*'. This will provide more legal certainty regarding the entities covered by the new scope.

— *Adopt* a new recital per which the Commission would carry out a public consultation on the application of the ePrivacy Directive to all private networks, with the input of the EDPS, Article 29 Working Party and other relevant stakeholders. Specify that as a result of the public consultation, the Commission should make any appropriate proposal to expand or limit the types of entities that should be covered by the ePrivacy Directive.

Processing of Traffic Data for Security Purposes

99. The EP first reading adopted Amendment 181 (Article 6.6(a)), authorising the processing of traffic data for security purposes. The Council's Common Position adopted a new version watering down some of the privacy safeguards. In this regard, the EDPS recommends that the EP and the Council:

— *Reject* this Article entirely because it is unnecessary and, if abused, could unduly threaten the data protection and privacy of individuals.

— Alternatively, if some variation of the current version of Article 6.6(a) is to be adopted, *incorporate* the data protection safeguards discussed in this Opinion (similar to those of the EP Amendment).

Actions for Infringements of the ePrivacy Directive

100. The Parliament adopted Amendment 133 (Article 13.6) giving legal entities the ability to bring legal action against infringements of any provisions of the Directive. Unfortunately the Council did not maintain it. The Council and EP should:

— *Endorse* the provision affording the possibility to legal entities, such as consumer and trade associations, the right to bring legal action against infringements of any provisions of the Directive (not only for infringement of the spam provisions as is the current approach in the Common Position and Amended Proposal). A greater diversity of enforcement mechanisms will encourage a higher level of compliance and effective application of the provisions of the ePrivacy Directive as a whole.

Meeting the Challenge

101. In all the above matters, the EP and Council must meet the challenge of devising proper rules and provisions that are both workable, functional and respect the rights to privacy and data protection of individuals. The EDPS is hopeful that the parties involved will do their utmost to meet this challenge and hopes that this Opinion will contribute in this endeavor.

Done at Brussels, 9 January 2009.

Peter HUSTINX
European Data Protection Supervisor

Opinion of the European Data Protection Supervisor on the proposal for a Council directive imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products

(2009/C 128/05)

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, and in particular its Article 41 [2],

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 sent to the EDPS on 14 November 2008,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 13 November 2008, the Commission adopted a proposal for a Council directive imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (hereinafter the proposal) [3].

2. The proposal aims at ensuring a high level of security of oil supply in the Community through reliable and transparent mechanisms based on solidarity amongst Member States, maintaining minimum stocks of oil or petroleum products and putting in place the necessary procedural means to deal with a serious shortage.

3. On 14 November 2008, the proposal was sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation (EC) No 45/2001. The EDPS welcomes the fact that he is consulted on this issue and notes that reference to this consultation is made in the preamble of the proposal, in accordance with Article 28 of Regulation (EC) No 45/2001.

4. Prior to the adoption of the proposal, the Commission informally consulted the EDPS on a specific article of the draft proposal (the current Article 19). The EDPS welcomed the informal consultation as it gave him an opportunity to make some suggestions prior to the adoption of the proposal by the Commission.

II. ANALYSIS OF THE PROPOSAL

General analysis

5. The current issue serves as a good illustration of the fact that there should be a constant awareness of the rules on data protection. In a situation which concerns Member States and their obligation to hold emergency oil stocks, which are owned mainly by legal entities, the processing of personal data is not very obvious, but, even though it is not envisaged as such, it can still take place. One should in any case consider the likelihood of personal data processing taking place and act accordingly.

6. In the current situation, there are basically two activities set out in the directive which could include the processing of personal data. The first is the collection by the Member States of information about the oil stocks and the subsequent transfer of this information to the Commission. The second activity relates to the power of the Commission to perform controls in the Member States. The collection of information about the owners of oil stocks could include personal data, such as the names and contact details of directors of the companies. This collection as well as the subsequent transfer to the Commission would then constitute the processing of personal data and would determine the applicability of either the national legislation implementing the provisions of Directive 95/46/EC or Regulation (EC) No 45/2001 depending on who is actually processing the data. Also granting the Commission a power to perform checks on emergency stocks in the Member States, which includes the power to gather information in general, could include the collection and therefore processing of personal data.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2008) 775 final.

7. During the informal consultation, which was restricted to the provision on the power of investigation of the Commission only, the EDPS advised the Commission to determine whether the processing of personal data in the context of a Commission investigation would only be incidental or would occur on a regular basis and serve the purpose of investigation. Following the outcome of this assessment two approaches were suggested.

8. If the processing of personal data was not envisaged and would therefore be purely incidental, the EDPS recommended to, first, explicitly exclude the processing of personal data as serving the purposes of the Commission investigation and, second, to state that any personal data which the Commission would come across in the course of the investigation would not be collected or taken into account and in case of accidental collection would immediately be destroyed. As a general backup clause the EDPS furthermore suggested to include a provision which stated that the directive would be without prejudice to the rules on data protection as laid down in Directive 95/46/EC and Regulation (EC) No 45/2001.

9. If, on the other hand, it was foreseen that data processing would take place on a regular basis in the context of a Commission investigation, the EDPS recommended the Commission to include a text which reflected the result of a proper data protection assessment. This should include the following elements: (i) the actual purpose of the data processing, (ii) the necessity of the processing of the data for achieving this purpose, and (iii) the proportionality of the data processing.

10. Although the EDPS' informal advice concerned the Commission's power of investigation only, his comments just as well applied to the other main activity explained in the proposed directive, namely collection and transfer to the Commission of information by the Member States.

11. The final proposal for a directive clearly shows that the Commission concluded that for the purposes of the directive no processing of personal data is envisaged. The EDPS is glad to see that his first suggested approach is fully reflected in the proposal.

12. The EDPS therefore expresses his support to the way in which the Commission assured compliance with data protection rules in the proposed directive. In the remainder of this advice only some detailed recommendations will be provided.

Comments on details

13. Article 15 of the proposed directive deals with the obligation on Member States to send to the Commission weekly statistical summaries of the levels of commercial stocks held within their national territory. Such information will normally contain little personal data. It could however contain information about the natural persons who own the oil stocks, or who work for a legal entity that owns the stock. In order to prevent the Member States from providing the Commission with such information paragraph 1 of Article 15 states that if Member States do so, they 'shall abstain from mentioning the names of the owners of the stocks concerned'. Although one should be aware of the fact that removing a name will not always result in data which cannot be retraced to a natural person, it looks as though in the current situation (statistical summaries of oil stock levels) this additional phrase will be sufficient to assure that no transfer of personal data to the Commission takes place.

14. The Commission's power of investigation is laid down in Article 19 of the proposed directive. The article clearly shows that the Commission has followed the first approach as explained in point 8 above. It states that processing of personal data may not be part of the checks carried out by the Commission. And even if the Commission comes across such data it may not be taken into account and must be destroyed in case of accidental collection. In order to align the wording with the wording used in the data protection legislation and prevent any misunderstanding, the EDPS recommends replacing the word 'gathering' in the first sentence by the word 'processing'.

15. The EDPS is satisfied to see that also a general backup clause on the relevant data protection legislation is included in the proposal. Article 20 clearly reminds the Member States as well as the Commission and other Community bodies of their obligations under Directive 95/46/EC and Regulation (EC) No 45/2001 respectively. The clause furthermore underlines the rights data subjects have under these rules, such as the right to object to the processing of their data, the right of access to their data and the right to have their data rectified in case of inaccuracy. One comment could perhaps be made on the positioning of this provision in the proposal. Because of its general nature, it is not restricted to the investigative power of the Commission only. The EDPS therefore recommends moving the article to the first part of the directive, for instance after Article 2.

16. Also in recital 25 reference is made to Directive 95/46/EC and Regulation (EC) No 45/2001. The objective of the recital is however rather unclear since it only mentions the data protection legislation as such and does not state anything further. The recital should clearly state that the provisions of the directive are without prejudice to the legislation mentioned. Furthermore, the last sentence of the recital seems to imply that the data protection legislation explicitly demands controllers to destroy data accidentally gathered immediately. Although it can be a consequence of the rules set out, such an obligation cannot be found in that legislation. It is a general principle of data protection that personal data are no longer kept than

necessary for the purposes for which they were collected or are further processed. If the first part of the recital is adjusted in the way just proposed, the last sentence has become superfluous. The EDPS therefore proposes to delete the last sentence of recital 25.

III. **CONCLUSION**

17. The EDPS wishes to express his support to the way in which the Commission assured compliance with data protection rules in the proposed directive.

18. At a detailed level the EDPS recommends the following:

— to replace the word 'gathering' in the first sentence of Article 19(1) by the word 'processing';

— to move Article 20, which is the general provision on data protection, to the first part of the directive, namely directly after Article 2;

— to add to recital 25 the message that the provisions of the directive are without prejudice to the provisions of Directive 95/46/EC and Regulation (EC) No 45/2001;

— to delete the last sentence of recital 25.

Done in Brussels, 3 February 2009.

Peter HUSTINX

European Data Protection Supervisor

IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS AND BODIES

COMMISSION

Euro exchange rates [1]

5 June 2009

(2009/C 128/06)

1 euro =

	Currency	Exchange rate		Currency	Exchange rate
USD	US dollar	1,4177	AUD	Australian dollar	1,7606
JPY	Japanese yen	137,48	CAD	Canadian dollar	1,5657
DKK	Danish krone	7,4472	HKD	Hong Kong dollar	10,9887
GBP	Pound sterling	0,87920	NZD	New Zealand dollar	2,2263
SEK	Swedish krona	10,9250	SGD	Singapore dollar	2,0530
CHF	Swiss franc	1,5191	KRW	South Korean won	1 768,65
ISK	Iceland króna		ZAR	South African rand	11,4189
NOK	Norwegian krone	8,9700	CNY	Chinese yuan renminbi	9,6871
BGN	Bulgarian lev	1,9558	HRK	Croatian kuna	7,3550
CZK	Czech koruna	27,003	IDR	Indonesian rupiah	14 078,75
EEK	Estonian kroon	15,6466	MYR	Malaysian ringgit	4,9556
HUF	Hungarian forint	289,10	PHP	Philippine peso	67,016
LTL	Lithuanian litas	3,4528	RUB	Russian rouble	43,5789
LVL	Latvian lats	0,7094	THB	Thai baht	48,464
PLN	Polish zloty	4,5420	BRL	Brazilian real	2,7345
RON	Romanian leu	4,2185	MXN	Mexican peso	18,7066
TRY	Turkish lira	2,1834	INR	Indian rupee	66,7910

[1] *Source*: reference exchange rate published by the ECB.

CORRIGENDA

Corrigendum to Interest rate applied by the European Central Bank to its main refinancing operations

(Official Journal of the European Union C 124 of 4 June 2009)

(2009/C 128/07)

On page 1 and on the cover page:

for: '1,00 % on 4 June 2009',

read: '1,00 % on 1 June 2009'.

2009 SUBSCRIPTION PRICES (excluding VAT, including normal transport charges)

EU Official Journal, L + C series, paper edition only	22 official EU languages	EUR 1 000 per year (*)
EU Official Journal, L + C series, paper edition only	22 official EU languages	EUR 100 per month (*)
EU Official Journal, L + C series, paper + annual CD-ROM	22 official EU languages	EUR 1 200 per year
EU Official Journal, L series, paper edition only	22 official EU languages	EUR 700 per year
EU Official Journal, L series, paper edition only	22 official EU languages	EUR 70 per month
EU Official Journal, C series, paper edition only	22 official EU languages	EUR 400 per year
EU Official Journal, C series, paper edition only	22 official EU languages	EUR 40 per month
EU Official Journal, L + C series, monthly CD-ROM (cumulative)	22 official EU languages	EUR 500 per year
Supplement to the Official Journal (S series), tendering procedures for public contracts, CD-ROM, two editions per week	multilingual: 23 official EU languages	EUR 360 per year (= EUR 30 per month)
EU Official Journal, C series — recruitment competitions	Language(s) according to competition(s)	EUR 50 per year

(*) Sold in single issues: up to 32 pages: EUR 6
from 33 to 64 pages: EUR 12
over 64 pages: Priced individually.

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

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

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

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

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

Sales and subscriptions

Priced publications issued by the Publications Office are available from our commercial distributors. The list of commercial distributors is available at:

http://publications.europa.eu/others/agents/index_en.htm

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

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

Publications Office
Publications.europa.eu

OFFICE FOR OFFICIAL PUBLICATIONS OF THE EUROPEAN COMMUNITIES
L-2985 LUXEMBOURG

EN