



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

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

¹ Council Document Nr. 9831/08, available at: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

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 guarantees².
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 service³.
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 matters⁴ 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

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, 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.

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.

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.

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 redress⁶. 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 actors⁷ 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 level⁸. 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

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, 01.05.2008. "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".

third state⁹. 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 trend¹⁰.

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 well¹¹ 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) 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 case¹² 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 Court¹³ 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 can not 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).

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.

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

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.

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

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.

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.

¹⁵ See Articles 11 and 13 of the DPF, mentioned in point 7 of this opinion.

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 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 letters¹⁶. 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

¹⁶ See footnote 2.

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 on the basis of specific criteria, and confirmed by decisions of the European Commission¹⁷. 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 Decision¹⁸ 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 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.

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.

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 from 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.

¹⁹ Chapter A. Binding international agreement, p. 8.

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. 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/EC²⁰. 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.

²⁰ - United Nations guidelines concerning computerized personal data files, adopted by the General Assembly on 14 December 1990, available at www.unhcr.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.

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 Party²¹. 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.
- 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.

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.

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 data²². 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 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 time²³.
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

²² See in particular Article 7 sub 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".

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.

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 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 Justice²⁴ 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 EC Directive 95/46, 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

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

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 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

(signed)

Peter HUSTINX
European Data Protection Supervisor