EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

Directorate D : Fundamental Rights and Citizenship
Unit D5 : Data Protection

SUMMARY REPORT:
EU-US INTERNATIONAL AGREEMENT ON PERSONAL DATA PROTECTION AND INFORMATION SHARING FOR LAW ENFORCEMENT PURPOSES
– INFORMAL CONSULTATION WITH DATA PROTECTION STAKEHOLDERS-
BRUSSELS, 2 FEBRUARY 2010

1. SUMMARY

Organised by the Data Protection unit D5 of Directorate General Justice Freedom and Security (DG JLS), this informal meeting of data protection stakeholders gathered ca. 50 representatives of data protection supervisory authorities, data protection officers (Eurojust, Europol), and national government departments in charge of data protection (e.g. Ministries of Justice, Ministries of Interior) as well as several JHA Counsellors and the Council Secretariat (Annex: Agenda).

Mr Aurel Ciobanu-Dordea, Director for Fundamental Rights and Citizenship at Directorate General Justice Freedom and Security (DG JLS) and Chair of the meeting, welcomed participants and explained the Commission's objective for this informal consultation of data protection stakeholders.

Mr Thomas Zerdick of the Data Protection unit D5 of DG JLS described the work that had been carried out so far by the High Level Contact Group on information sharing and privacy and personal data protection (HLCG): the HLCG had been established by the EU-US Justice and Home Affairs Ministerial Troika on 6 November 2006. It had presented a public final report on 28 May 2008 and an addendum to this report on 28 October 2009 which identified a set of core privacy and data protection principles as well as related issues pertinent to the EU-US transatlantic relationship[1], pointing to the negotiation of a binding international agreement as the next step forward. It also covered the new responsibilities and obligations for the protection of personal data conferred upon the EU by the Lisbon Treaty.

Mr Luigi Soreca, Head of Unit of the External Relations unit A2 of DG JLS, highlighted that in the 2009 Stockholm Programme the European Council had invited the Commission to propose a "recommendation for the negotiation of a data protection and, where necessary, data sharing agreement for law enforcement purposes with the US, building on the work carried out by the EU-US High Level Contact Group on data protection" and the European Parliament had equally called for an EU-US agreement ensuring adequate

[1] Council Document 15851/09 ; http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf

protection of civil liberties and personal data protection. He explained that an online public consultation has been recently launched (28 January 2010) and presented the envisaged process leading to the negotiation of a future EU-US international agreement, with dedicated meetings with data protection stakeholders, private sector stakeholders and police and judiciary stakeholders as well as informing the European Parliament in February and March 2010.

Ms Marie-Hélène Boulanger, Head of Unit of the Data Protection unit D5 of DG JLS, presented the non-exhaustive discussion paper prepared by the Commission (Annex: Discussion Paper), formulated in a deliberately open way to elicit a broad range of constructive comments.

In short, a consensus emerged from the participants in the discussions that a legally binding EU-US framework agreement on personal data protection based on the HLCG data protection principles was welcome in general but would always need to be complemented by specific agreements with specific data protection provisions, and as such, a framework agreement could not by itself be the legal basis for any data transfers from the EU to the US. Participants were divided on the question of whether the material scope of the agreement should be defined narrowly to encompass police and judicial cooperation in criminal matters only or whether it should also include the use of visa, asylum and immigration data for law enforcement purposes. A majority spoke in favour of the agreement covering private to government and government to government data transfers. A majority of participants favoured the idea that the agreement should apply to existing and future EU and EU Member States' bilateral agreements with the US, though some participants acknowledged that extending the scope to existing agreements might prove difficult in practice and may only be achieved over time. Moreover, participants commented on further elements of a future agreement (e.g. non-discrimination, judicial redress), and pointed to other subjects in addition to those addressed by the HLCG (e.g. data minimisation, liability, time limits to data retention and others).

The Commission invited all participants to submit written contributions by 12 March 2010 (coinciding with the end of the public consultation) to the e-mail address of the public consultation provided for on:

http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0005_en.htm.

2. DETAILS OF THE DISCUSSION

A. Purpose of the Agreement

As to the questions on the purpose of the agreement, there seemed to be an agreement amongst the attendees that a **general agreement could not constitute the legal basis of each data transfer** and should therefore not be drafted as a data sharing agreement, but rather a **general agreement on data protection principles** which would apply to all personal data processing acts in relations between EU and US. However, such an agreement would always need to be complemented by specific agreements with specific data protection provisions which should not deviate from or make limitations to the general agreement. Some attendees pointed out that the EU already had its data protection principles enshrined in the acquis and underlined the need for an **enforceable agreement**, retaking the HLCG principles but further translated into technically workable principles in practice.

B. Scope of the Agreement

– Questions B1, B2, B3

Addressing the questions on **material scope**, participants were divided on the question of whether the material scope of the agreement should be defined narrowly to encompass judicial cooperation in criminal matters (Chapter 4) and police cooperation (Chapter 5) only or whether it should also include visa, asylum and immigration data when processed for law enforcement purposes. There was considerable agreement **not to include civil law cooperation** in such a general agreement, given the different principles by which it was governed.

In any case, the agreement should come to a common definition of which law enforcement authorities are targeted by this agreement. It was flagged that such a common definition might be hard to achieve, given the existing inner disparities already within the EU with some MS including border and tax control as law enforcement tasks.

Similarly, doubt was cast by some attendees on whether data processing for national security should be included in the agreement or not.

– Questions B.4, B.5, B.6

Concerning the **personal scope** of the agreement, a majority spoke in favour of the agreement covering private to government and government to government data transfers when processed for the prevention and prosecution of crimes given the current reality of such data being used for law enforcement goals (e.g. PNR, TFTP). There was some disagreement between attendees on whether to impose similar data protection obligations on private entities as on public authorities. It was suggested that the agreement could however impose similar obligations on public entities, independently of whether the personal data originated in the public or the private sphere.

As to the **list of law enforcement authorities**, it was perceived that a description of the different kinds of activities of law enforcement authorities was preferable to drawing up an exhaustive list of all EU and US law enforcement authorities to be covered.

– Question B.7

Addressing the question of **relationship with other agreements**, the majority of attendees preferred that the agreement should apply to both existing and future EU (including agencies and bodies) and EU Member States' bilateral agreements with the US, though some participants acknowledged that extending the scope to existing agreements might prove difficult in practice and may only be achieved over time.

Some attendees warned that it might be unwise to renegotiate data protection aspects of earlier agreements because this might result in the lowering of standards instead of the other way around, depending on the outcome of the negotiations.

C. Nature of the Agreement

– Questions C.15, C.16

Raising the question of nature of the agreement, attendees reiterated that the agreement should not be a data sharing agreement but that it should only encompass the principles with which all personal data processing acts in EU-US relations should comply.

'Reciprocity' being understood to mean granting the same data protection level to US and non-US data subjects was regarded as an important part of the agreement.

D. Data protection principles

– Question D.1

Most attendees advocated the **inclusion of specific data protection rules** for specific data categories (genetic data, biometric data) into the agreement, complementing the general data principles for personal data protection.

– Question D.2

There was wide agreement on the inclusion of a joint review mechanism similar to PNR/TFTP/Schengen exercise. An "eminent person" approach was judged not being satisfactory. Attendees stressed that the DPAs should be involved as much as possible in such a joint review, to strengthen data subjects' data protection rights with detailed rules on how the joint review mechanism would work in practice. Some pointed out that 'accountability' is not an EU data protection principle as such (but: 'responsibility') and has different meanings in different jurisdictions.

– Question D.3

As to individual access, it was put forth by the majority of attendees that indirect access could be a limited exception to the data subjects' right of direct access (see Art. 8 EU Charter) and that no exceptions to indirect access should be allowed. It was further specified that independence of the data protection supervisory authority indirectly accessing the personal data on behalf of the data subject was of utmost importance and that access should be guaranteed regardless of the nationality of the data subject. Some attendees flagged that the USA allegedly only operate a direct access system, with certain exemptions.

– Question D.4

Addressing the issue of a single contact point, a vast majority of attendees cast doubt on the use of including the principle of a single contact point in a general agreement as it was unclear what his or her tasks would be. Others flagged that a data subject would need to get in touch with the controller first, and such contact would be different from the right to contact the data protection supervisory authority. According to some, the US system may have difficulties in establishing a single contact point, given that there are different legal acts governing data protection, unlike the unified legal framework known in Europe.

– Question D.5

As to the allowance of onward transfer, attendees advocated a strong general principle restricting onward transfer as much as possible and that 'legitimate public interest' should be well defined.

– Question D.6

Addressing the question of possible cooperation mechanisms between US and EU data protection supervisory authorities and/or judicial authorities in criminal matters, it was generally perceived to be too early to address this as in the US currently there is no independent data protection supervisory authority in place.

– Question D.7

Regarding judicial redress, attendees underlined the importance of this principle and were of the opinion that the general agreement should lay down the general principle of effective judicial redress, irrespective of the nationality or residence of the data subject. It would be up to the USA then to adapt its domestic legal system to ensure application of this data protection principle.

E. Others

– Questions E.25-26-27

Attendees proposed further safeguards to be included in the framework agreement: specified data retention periods, together with a liability clause, also for data security including the right to (financial) compensation; information to data subjects in cases where their data has been corrected or erased; the principle of data minimisation and addressing the issue of profiling.

Some attendees did not favour strict data retention principles in a general agreement from a practical point of view and thought it would be better to reserve that for the specific agreements.

Attendees thought it was better to revise the question of the duration of the agreement once the outcome of the negotiations was known. In general, a longer duration was preferred given that the agreement contained data principles which should always apply.

Attendees thought including real sanctions might be difficult but a sort of dispute resolution procedure should be included in the agreement. Some found an explanatory memorandum of the HLCG principles necessary.

Responding to a question whether the documents of the HLCG could be translated into the EU languages, the Commission said it would refer the request for translation to the Council and told the attendees it would later on circulate a summary report of the meeting.

Annexes:

– Agenda of the meeting
– Stakeholder discussion paper

Contact:
Thomas Zerdick, Telephone:(32-2) 298 50 98, thomas.zerdick@ec.europa.eu

* * *

Data protection expert meeting

– Meeting, 2 February 2010 –

10:00 hrs to 17:00 hrs
Centre Borschette, Room 0C (36 rue Froissart, 1040 Brussels)

Agenda

Chair:

Mr Aurel CIOBANU-DORDEA, Director,
Directorate D : Fundamental Rights and Citizenship,
DG Justice, Freedom and Security, EU Commission

1. Introduction by the Commission (*Chair*)
2. A future EU-US international agreement on personal data protection and information sharing for law enforcement purposes:
   - Presentation by the Commission on the work by the High Level Contact Group on information sharing and privacy and personal data protection (HLCG) (*D5*)
   - Presentation by the Commission on the debate for a future "EU-US international agreement on personal data protection and information sharing for law enforcement purposes". (*A2*)
3. Discussion with the data protection experts on the guiding principles of such an agreement.
4. The way forward.
5. Any other business.

* * *

Discussion paper

Future EU-US international agreement on personal data protection and information sharing for law enforcement purposes

Background:

1. Law enforcement authorities on both sides of the Atlantic collect and process personal data in order to prevent, detect and prosecute crime and terrorism. The processing and transfer of personal data is considered an essential element of transatlantic law enforcement cooperation in order to fight serious transnational crime and terrorism effectively. Consequently the protection of personal data in the context of the processing and transfer of data for law enforcement purposes has been the subject of discussions and negotiations of international agreements between the European Union and the United States of America (US) over the past years.[2]

2. A High Level Contact Group on information sharing and privacy and personal data protection (HLCG) was established by the EU-US Justice and Home Affairs Ministerial Troika on 6 November 2006 to discuss privacy and personal data protection in the context of the exchange of information for law enforcement purposes as part of a wider reflection on how to best prevent and fight terrorism and serious transnational crime. The goal of this group was to explore ways enabling the EU and the US to work more closely together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed. The HLCG presented a final report on 28 May 2008 and an addendum to this report on 28 October 2009 which identified a set of core privacy and data protection principles and a set of related issues pertinent to the EU-US transatlantic relationship[3]. The non-binding reports have been welcomed at EU-US JHA Ministerial Troika meetings[4] and EU-US Summits[5], pointing to the negotiation of a binding international agreement as the next step forward.

---

[2] US-Europol cooperation agreements: http://www.europol.europa.eu/legal/agreements/Agreements/16268-2.pdf; http://www.europol.europa.eu/legal/agreements/Agreements/16268-1.pdf; US-Eurojust agreement: http://www.eurojust.europa.eu/official_documents/Agreements/061106_EJ-US_co-operation_agreement.pdf; 2007 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), OJ L 204 of 4.8.2007, p. 16; Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, OJ L 8 of 13.1.2010, p. 9

[3] http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf

[4] Joint statement of 28 October 2009: http://register.consilium.europa.eu/pdf/en/09/st15/st15184.en09.pdf

3. The European Council invites the Commission in the Stockholm Programme[6] to propose a recommendation for the negotiation of a data protection and, where necessary, data sharing agreement for law enforcement purposes with the US, building on the work of the HLCG.

4. The European Data Protection Supervisor presented an opinion on the HLCG 2008 report on 11 November 2008[7].

5. This paper non-exhaustively lists questions on which the Commission wishes to seek the opinion of stakeholders with a view to a future EU-US agreement on personal data protection and information sharing for law enforcement purposes.

A. Purpose:

6. What should be the purpose(s) of the agreement? Should the agreement establish data protection standards for EU-US law enforcement cooperation? Or should it address also wider issues related to the processing and transfer of personal data in the context of transatlantic law enforcement cooperation, e.g. reciprocity of information transfer or impact on relations with other third countries?

7. Should the agreement itself be a legal basis for transfer of personal data for law enforcement purposes? Or should there *always* be an additional, specific agreement regulating the transfer of personal data for a particular law enforcement purpose?

B. Scope of the agreement

Material scope

Question B1:

8. Should the agreement cover personal data protection when information is transferred under Title V of the Treaty on the Functioning of the European Union (the TFEU) in the area of police cooperation (Chapter 5)? Should it also cover information transferred in the course of judicial cooperation in criminal matters (Chapter 4)? Should it also be applicable to the transfer of personal data in the context of other

---

[5] 2008 EU-US Summit: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/er/101043.pdf; 2009 EU-US Summit: http://ec.europa.eu/external_relations/us/sum11_09/docs/declaration_en.pdf

[6] http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf

[7] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf

Union policies within the area of freedom, justice and security, i.e. the security elements of immigration, visa, asylum and civil law cooperation?

Question B2:

9. Should there be a common definition of law enforcement purpose[8]?

---

[8] Note the differences between the EU and the US in the definition of "law enforcement purposes", cf. the May 2008 HLCG Final Report. For the EU, law enforcement purposes refer to "the prevention, detection, investigation or prosecution of criminal offences". For the US, the interpretation of law enforcement goes beyond criminal offences and includes "border enforcement, public security and national security purposes".

Note past examples of describing the remit of law enforcement cooperation: "enhance cooperation in preventing, detecting, suppressing, and investigating criminal offences within the respective jurisdictions of the parties, in particular by facilitating the reciprocal exchange of information, including personal data" (like in the Europol-US supplemental agreement on the exchange of personal data and related information) or "enhancing cooperation in combating serious forms of transnational crimes including terrorism" (like in the Eurojust-US agreement) or "improve cooperation between the competent authorities in preventing and combating serious forms of international organised crime (along the lines of the Interpol-Europol agreement). Should any of these be used as a model?

Question B3:

10. Should the agreement explicitly exclude the processing and transfer of data for national security purposes from its scope?

Personal scope

Question B4:

11. Should the agreement only cover government-to-government transfers of information? Or should it also be applicable to transatlantic transfers of personal data from private entities to law enforcement authorities? If so, should the conditions on private – public data transfers be in any way different from the government-to-government transfers?

Question B5:

12. Should the agreement qualify or list the US Federal law enforcement authorities eligible to receiving information?

Question B6:

13. Should the agreement be applicable to the protection of personal data and information transfers to the US by law enforcement authorities of EU Member States *in general* or only by *specific* law enforcement authorities of Member States? If the latter, which ones? Should the agreement be applicable to the protection of personal data and information transfers to the US by bodies or agencies of the Union *in general* or only apply to *specific* bodies and agencies? If the latter, which ones?

Relationship with other agreements

Question B7:

14. What should be the legal relationship between the agreement and already existing agreements (e.g. 2007 EU-US PNR Agreement, EU-US TFTP agreement, Europol-US agreement, Eurojust-US agreement, EU-US mutual legal assistance agreement, bilateral EU Member States' agreements with the US)? What shall be the legal relationship between this agreement and future EU-US agreements or arrangements and bilateral agreements and arrangements concluded with US?

C. Nature of the agreement:

15. Should the agreement include a provision to the effect that EU and US law enforcement authorities may request from each other the same types/categories of information and personal data (reciprocity)?

16. Should the data protection standards envisaged by the agreement always be applicable for transatlantic law enforcement cooperation as a minimum set of rules?

D. Data Protection Principles

Question D1: General and specific principles?

Should it include only general data protection principles or also specific data protection principles tailored to different categories of data?

Question D2: Accountability

17. Should the agreement provide for modalities and consequences of "accountability", e.g. internal and external review procedures? Should the agreement notably provide for a joint review mechanism?

Question D3: Individual Access

18. Should the agreement spell out the conditions for the right to access? If there is no possibility to directly access one's own personal data for justified reasons, should the agreement provide for the possibility of indirect verification through an independent authority responsible for the oversight of the processing in the sending or recipient country?

Question D4: single contact points

19. Should the agreement provide for a single contact point in the US in case of data protection concerns related to data transferred from the EU? Should the agreement provide for a single contact point in the EU in case of data protection concerns related to data transferred from the US?

20. Should the modalities for transparency and assistance to data subjects by US and EU data protection supervisory authorities be spelled out in the agreement?

Question D5: Restrictions on onward transfers to third countries or international bodies

21. Should the agreement allow for onward transfers? If yes, under which conditions? Should the agreement provide for clarification on the definition of "legitimate public interests" allowing for an onward transfer?

Question D6: cooperation mechanisms

22. Should the agreement provide for cooperation mechanisms between US and EU data protection supervisory authorities? If yes, please specify.

23. Should the agreement provide for cooperation mechanisms between US and EU judicial authorities in criminal matters, in particular courts and tribunals? If yes, please specify.

Question D7: judicial redress

24. Should the agreement lay down provisions for effective judicial redress for data subjects? How could this be achieved? Should laws which discriminate in respect of access to the courts on grounds of nationality or residence be amended?

E. Others

25. What further safeguards for data subjects shall be included in the agreement?

26. Should the agreement be concluded for an undetermined or determined period? In the later case, how long should the agreement last?

27. What procedures and sanctions should the agreement provide for in case of non-compliance other than suspension and termination?

22.1.2010