COMMISSION EUROPÉENNE
Secrétariat général
COM(2010) 252/2
Annexe au document COM(2010) 252 PO/2010/3091
RESTREINT UE

PROPOSITION DE RECOMMANDATION DU CONSEIL AUTORISANT L'OUVERTURE DE NEGOCIATIONS EN VUE D'UN ACCORD ENTRE L'UNION EUROPEENNE ET LES ETATS-UNIS D'AMERIQUE SUR LA PROTECTION DES DONNEES PERSONNELLES LORS DE LEUR TRANSFERT ET DE LEUR TRAITEMENT A DES FINS DE PREVENTION, D'INVESTIGATION, DE DETECTION OU DE POURSUITE D'ACTES CRIMINELS Y COMPRIS LE TERRORISME, DANS LE CADRE DE LA COOPERATION POLICIAIRE ET JUDICIAIRE EN MATIERE PENALE

EXPLANATORY MEMORANDUM

1. The European Union (EU) and the United States of America (US) share fundamental values of freedom, democracy, rule of law and human rights. Moreover, the US is a major Strategie partner of the EU in the fight against crime and terrorism.

2. Law enforcement authorities on both sides of the Atlantic collect and process personal data in order to prevent, detect, investigate and prosecute criminal and terrorist acts. Processing and transferring personal data is considered an essential part of fighting crime and terrorism effectively, both within the European Union and when cooperating with international partners.

3. Since the terrorist attacks of 11 September 2001 in the US and subsequent attacks in Europe and other parts of the world, the EU has enhanced police and judicial Cooperation in criminal matters with the US. This has led, *inter alia,* to conclusion of several agreements[1]. They include clauses on protection of personal data when information is processed and transferred for the purposes of preventing, investigating, detecting and prosecuting criminal offences, including terrorism.

4. The EU and the US share similarities in their approaches to personal data protection, but there are also differences which rendered negotiation of the aspects of the aforementioned agreements addressing protection of personal data and privaey particularly difficult.

5. In order to improve mutual knowledge of the rules on personal data protection and privaey in the context of transatlantic police and judicial Cooperation in criminal matters, an EU-US expert group called the High-Level Contact Group on Information-Sharing and Privaey and Personal Data Protection (HLCG) was established by the EU-US Justice and Home Affairs Ministerial Troika on 6 November 2006. Its aim was to discuss privaey and personal data protection in the context of exchanges of information for law enforcement purposes as part of a wider reflection on the best approach to prevent and fight terrorism and serious transnational crime. The remit of this group was to explore ways of enabling the EU and the US to work together more closely on exchanging law enforcement information, while guaranteeing protection of personal data and privaey.

6. The HLCG presented a final report on 28 May 2008 followed by an addendum on 28 October 2009. These identified a set of core privaey and data protection principles along with related issues pertinent to the EU-US relationship . The reports were welcomed at meetings of the EU-US Justice and Home Affairs Ministerial Troika[3] and EU-US

summits[4], paving the way for negotiation of a binding international agreement as the next step forward.

7. In the Stockholm Programme[5] the European Council 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' ('the agreement')-

8. The European Parliament has, in turn, called for an EU-US agreement ensuring adequate protection of civil liberties and personal data[6].

9. A consultation process was launched in early 2010 as part of the preparatory work for this recommendation. A public consultation was posted on the 'Your voice in Europe' website on Europa from 28 January to 12 March 2010. 77 responses were received, two thirds of which were from Citizens, 22 from organisations and 4 from public authorities. Amongst Citizens, the general sentiment was concern about increased data-sharing or, indeed, about sharing any data at all, There was some scepticism about the security of data when transferred and processed and about the subsequent use made of it by US authorities. The overwhelming plea from organisations was for clarity — of terms, obligations and procedures — and also as regards how the agreement will fit in with existing agreements. An agreement that improved legal certainty and removed discrepancies between the two legal systems would be welcome. In general, organisations favoured a broad scope but were divided on the issue of transfers from private entities to police and judicial authorities. The responses from public authorities were detailed. They emphasised the importance of the agreement having a wide scope but clear and limited purpose, establishing binding, legally enforceable data protection standards relating to data transfers for law enforcement purposes only. The agreement should establish standards at least equivalent to those already set at European level! and should contain principles that will apply to existing and future agreements, including bilateral ones. The replies and a summary are available on the website of the Commission's Directorate-General for Justice, Freedom and Security[7].

10. Moreover, meetings on this subject with data protection, private-sector, police and judiciary stakeholders were held in February and March 2010.

11. The meeting with the data protection stakeholders, representing national and European data protection supervisory authorities, data protection officers (Eurojust and Europol) and government departments in charge of data protection (Ministries of Justice and of the Interior) produced a consensus that a legally binding EU-US framework agreement on personal data protection based on the HLCG data protection principles was welcome. It would need to be complemented by more detailed agreements with specific data protection provisions, 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 whether the material scope of the agreement should be defined narrowly to restrict it to police and judicial cooperation in criminal matters only or should also extend to use of visa, asylum and immigration data for law enforcement purposes. The majority of participants were in favour of the agreement covering private-to-government and government-to-government data transfers. Most favoured the idea that the agreement should apply to existing and future bilateral agreements between the EU and individual EU Member States and the US, though some acknowledged that extending the scope to existing agreements might prove difficult in practice and might only be achieved over time. Participants also commented on further aspects of a future agreement (e.g. non-discrimination and judicial redress) and

pointed to other subjects in addition to those addressed by the HLCG (data minimisation, liability, time limits on data retention and others).

12. Participants in the meeting with representatives of the private sector, including airlines, banks, security and telecommunications companies and advocacy groups, likewise favoured a narrow scope for the agreement, limited to data protection principles. There was concern about exposure to (additional) requests or obligations from police authorities and strong demand for a well defined data privacy framework in the event of transfers of personal data between the EU and the US for the purposes of preventing and fighting crime and terrorism. Transparency, notice to data subjects, access to data and redress were highlighted as particularly important aspects. There was also concern about direct transmission to the US, for law enforcement purposes, of personal data originally gathered for commercial purposes by the private sector.

13. A meeting with police and judicial stakeholders was held on 10 March 2010. Participants favoured a narrow scope for the agreement, limited to data protection principles. The majority were also in favour of covering visa, asylum and immigration data transferred for law enforcement purposes. From a law enforcement perspective, there are no watertight borders between police cooperation, judicial cooperation and use of visa, asylum and immigration data for law enforcement purposes. Including civil law cooperation was considered premature. The majority were also in favour of the agreement covering private-to-government and government-to-government data transfers. On judicial redress in the US, different approaches were taken, ranging from concentrating on indirect redress to a cooperation mechanism between the EU and the US, via the EU aiming to set 'goal-based standards' where the US would have to look for solutions to ensure judicial redress in the agreement. Participants favoured the idea that the agreement should be without prejudice to existing EU and bilateral agreements with the US or to international agreements to which the US and Member States are party (including at UN level), clearly signalling that existing agreements should be considered *'acquis'*. Europol and Eurojust stressed their authority to conclude international agreements but were Willing to consider adaptations if the agreement provided higher standards than their bilateral agreements with the US.

***

14. In the light of the foregoing, the Commission considered the various policy options for further action. 'Doing nothing' was not considered viable since the legal uncertainties described would persist. As the consultations have shown, concerns would still be voiced about the insufficient legal framework for protecting personal data when transferred from the EU to the US and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, notably because of differences regarding the scope of restrictions or exemptions to privacy rights, non-discriminatory access to the courts and independent public supervision. The aforementioned European Parliament resolution points in the same direction. A non-binding agreement (e.g. an exchange of letters) would also fail to dispel the legal uncertainties.

15. The Commission considers the US's accession to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and to its Additional Protocol with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No 181) a desirable Step. This option would be generally beneficial for protection of personal data transferred between the EU and the US because the Convention is open for accession by non-Council of Europe Member States, has been ratified by all EU Member States and provides a recognised international standard made up of legally binding data protection principles. However, the Convention allows derogations from the basic principles

governing data protection in the context of data processing for police, State security or crime suppression purposes, the very purposes for which the European Union is contemplating an agreement with the US. While the US's accession to the Council of Europe Convention and its Additional Protocol is a desirable goal that should be pursued, it would not be sufficient to address the issues raised.

16. In the Commission's view, and in line with the broad consensus of the consultations, a legally binding agreement would therefore be the preferred option to provide legal certainty. Ideally, the agreement should lay down high data protection standards for transferring and processing personal data for the purpose of preventing, investigating, detecting or prosecuting criminal offences which provide effective rights for the data subject. Such an agreement is also considered advantageous for competent public authorities because it would provide a complete, self-contained and agreed set of data protection standards which by itself would bring added value for transatlantic cooperation in fighting crime, including terrorism. It is for that reason that the Commission proposes a personal scope encompassing European Union institutions, bodies, offices and agencies, European Union Member States and US public authorities and a wide temporal scope of the agreement so as to establish a single reference framework for transatlantic data transfer for the purposes of police and judicial cooperation in criminal matters. Such approach was supported notably by data protection experts. Moreover, the agreement shall apply to data transfers and processing concerning criminal intelligence[8] but not to those concerning essential national security interests and specific intelligence activities in the field of national security because matters of national security remain the sole responsibility of the Member States. National security interests will have to be defined narrowly in order not to unduly limit the scope of the agreement.

***

The aims of the future EU-US agreement should be fourfold:

- The agreement should ensure a high level of protection of the fundamental rights and freedoms of individuals, in particular the right to protection of personal data, in line with the requirements of the Charter of Fundamental Rights of the European Union ('the Charter') and the Treaty of Lisbon, when personal data are transferred between the EU and the US and processed for the purpose of preventing, investigating, detecting or prosecuting crime, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters.

- The agreement should provide a clear and coherent legally binding framework of personal data protection standards that must be met when personal data are transferred between the EU and the US and processed for the aforementioned purposes. Such a framework should remove the uncertainties and bridge the gaps in protection created in the past because of significant differences between EU and US data protection laws and practices. The agreement itself should therefore provide enforceable data protection standards and establish mechanisms for implementing them effectively. The latter may imply additional costs for public authorities in view of additional assistance and supervision tasks.

- The agreement should provide a high level of protection for personal data transferred to and subsequently processed in the US for the purpose of preventing, investigating, detecting or prosecuting criminal offences, taking into account the specifies of police and judicial cooperation in criminal matters and also of the US legal system. These imply placing some limitations or restrictions on the rights of data subjects which, due to the specific characteristics of the matter, should be limited to criminal and judicial proceedings. It therefore follows that it would not be desirable to widen the scope of the future agreement to administrative proceedings.

- The agreement would not do away with the requirement for a specific legal basis for transfers of personal data between the EU and the US, with specific data protection provisions tailored to the particular category of personal data in question. Nonetheless, the agreement should facilitate police and judicial cooperation between the EU and the US, including transfers of personal data for the purpose of preventing, investigating, detecting or prosecuting crime, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters. It would guarantee a high level of protection of personal data for such transfers, thereby building trust in the legal framework governing them.

Article 7 of the Charter enshrines the fundamental right to respect for private and family life. Article 8 of the Charter enshrines the fundamental right to protection of personal data of every individual and defines the basic principles for protection of personal data, which include the data subject's right of access and control by an independent authority. Article 47 of the Charter provides for the right to an effective remedy and to a fair trial. The Charter has the same legal force as the Treaties pursuant to Article 6(1) of the Treaty on the European Union (TEU). Moreover, pursuant to Article 6(3) of the TEU, the fundamental rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) constitute general principles of European Union law. Article 8 of the ECHR also enshrines the right to respect for private and family life. Furthermore, the newly introduced Article 16 of the Treaty on the Functioning of the European Union (TFEU) provides for protection of personal data in the EU. On that basis, the European Parliament and the Council are empowered to adopt — as co-legislators — rules on processing of personal data by EU institutions, bodies, offices and agencies and by the Member States when carrying out activities which fall within the scope of EU law along with rules governing the free movement of such data.

19. In addition to EU primary law and relevant case law of the European Court of Justice and the European Court of Human Rights, EU secondary legislation on protection of personal data constitutes the benchmark for the data protection Standards in the agreement. This EU *acquis* needs to be taken fully into account, notably: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[9]; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic Communications sector[10]; Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial Cooperation in criminal matters[11]; and Regulation (EC) No 45/2001 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[12].

20. Other international instruments on protection of personal data are also important reference documents, in particular: the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) and its Additional Protocol with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181); Recommendation No R(87) 15 regulating the use of personal data in the police sector; the United Nations guidelines concerning computerised personal data files; and the Organisation for Economic Cooperation and Development Recommendation concerning guidelines governing the protection of privacy and transborder flows of personal data.

21. The HLCG laid the ground by identifying a set of data protection principles and related issues. The objective of the HLCG was to identify common features between the EU and US frameworks for protection of personal data. The negotiations with the US should build on the HLCG principles but not be limited to them because they are not sufficient in themselves. The principles are worded in a very general way and would benefit from further elaboration to spell out in more detail how they should be implemented effectively

in practice. Moreover, terminology used in the HLCG principles leaves room for Interpretation by either side and therefore requires clarification. Finally, additional issues, e.g. liability and compensation, also need to be addressed in the agreement. This assessment was confirmed in the consultation process, during which the need for fine-tuning the HLCG data protection principles and adding other essential data protection principles was stressed repeatedly. The final result of the negotiations should be in line with the Union's personal data protection standards described above.

22. The envisaged agreement should be based on Article 16 of the TFEU, in conjunction with Article 216 thereof.

23. In line with Article 218 paragraph 3 of the TFEU, the Commission should be nominated as the Union negotiator.

24. In line with Article 218 paragraph 10 of the TFEU, the European Parliament should be immediately and fully informed at ail stages of the procedure.

* * *

25. The Commission therefore recommends that the Council authorise the opening of negotiations with the United States of America for an agreement, based on Article 16 of the TFEU on protection and free movement of personal data, when personal data are transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters within the scope of Chapter 4 or 5 of Title V of Part Three of the TFEU.

US-Europol Cooperation Agreement:
http://www.europol.europa.eu/Iegal/agreements/Agreements/I6268-2.pdf;; US-Eurojust agreement: http://www.eurojust.europa.eu/official_documents/Agreements/061I06JBJ-US_cooperation_agreement .p d f;
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, 4.8.2007, p. 16;
Agreement on mutual legal assistance between the European Union and the United States of America (OJL 181, 19.7.2003, p. 34).
http://register.consilium.europa.eu/pdf/en/09/stl5/stl5851 .en09.pdf.
Joint Statement of 28 October 2009:
http://register.consilium.europa.eu/pdf/eny09/stl5/stl5184.en 09.pdf. 2008 EU-US Summit:
http://wwwxonst!îum.europa**.eij**/uedocs/cms_Data/docs/pressdata/ep/er/î 01043 .pdf; 2009 EU-US Summit: http://ec.europa.eu/external_relations/us/sumî
î_09/docs/declaration_en.pdf.
http://register.consilium.europa.eii/pdf/en/09/stl7/stl7024.en09.pdf.
Cf. Resolution 2008/2 Ï99 of March 2009; most recently, recommendation of the Committee on Civil Liberties, Justice and Home Affairs of 5 February 2010, doc. A7-0013/2010.
http://ec.europa.eu/justice_home/news/consuiting_public/news_consulting__0005_en.htm.
Cf. Article 2(c) of the Framework Décision 2006/96O/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89).
OJ L281, 23.11.1995, p. 31.
OJ L 201, 31.7.2002, p. 37, as amended by Directive 2009/136/EC of the European Parliaraent and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Régulation (EC) No 2006/2004 on coopération between national authorities responsable for the enforcement of

consumer protection Iaws (Text with EEA relevance) (OJ L 337, 18.12.2009, p. 11). O J L 350, 30.12.2008, p. 60. O J L 8, 12.1.2001,p. 1.

Proposal for a **COUNCIL RECOMMENDATION**

to authorise the opening of negotiations for an agreement between the European Union and the United States of America on protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters

In the light of the foregoing considerations, the Commission recommends that the Council:

- authorises the Commission to negotiate with the United States of America for an agreement, based on Article 16 of the TFEU on protection and free movement of personal data, when personal data are transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters within the scope of Chapter 4 or 5 of Title V öo Part Three of the TFEU;

- issues the annexed negotiating directives;

- designates a special committee, in consultation with which the negotiations must be conducted.

RESTREINT UE

NEGOTIATING DIRECTIVES

The Commission shall, in the course of negotiations, aim to achieve the specific objectives set out in detail below [while reflecting, to the extent practicable, the recommendations made by the European Parliament in its Resolution ###] :

1. The purpose of the Agreement shall be to ensure a high level of protection of the fundamental rights and freedoms of individuals when personal data are transferred and processed to and by competent public authorities of the European Union and its Member States and the US for the purpose of preventing, investigating, detecting or prosecuting crime, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union. it shall lay down legally binding arid enforceable data protection standards for such processing and establish mechanisms to ensure effective application' of those standards in practice.

2. The Agreement shall provide for a high level of data protection standards in line with the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union, the European Convention for the Protection of Human Rights and Fundamental Freedoms and EU secondary legislation for the protection of privacy and

personal data. The Agreement shall, in particular: ensure protection of everyone's personal data, regardless of nationality or place of residence; provide that such data must be processed fairly for specified purposes and on a legitimate basis laid down by law; stipulate that everyone has the right of access to data which have been collected concerning Mm or her, including the right to have them rectified; and guarantee that compliance with these rules shall be subject to control by an independent public authority, in line with Article 8 of the Charter of Fundamental Rights of the European Union.

3. The Agreement shall explicitly State that it creates enforceable rights for data subjects.

4. The Agreement shall apply to all future EU or Member States personal data transfer and processing agreements with the US for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters. The Agreement shall also apply to ail existing EU or Member States personal data transfer and processing agreements with the US for the purpose of preventing, investigating, detecting or prosecuting, criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters after a transitional period of three years. In this respect the Agreement shall place an obligation on the EU and the US to bring those agreements in conformity with the Agreement no later than three years after its entry into force.

5. The Agreement shall explicitly state that it cannot be the legal basis for any transfers of personal data, including from private entities, between the European Union and the US and that a specific legal basis for such data transfers shall always be required.

6. The Agreement shall apply to transfers and processing of personal data to and by European Union institutions, bodies, offices and agencies, European Union Member States and US public authorities responsible for prevention, investigation, detection or prosecution of criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters. It shall apply to the aforementioned transfers and processing regardless of where the personal data originate from, as long as the personal data are processed by a competent public authority for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism.

7. The Agreement shall build on the data protection principles identified by the High-Level Contact Group on Information-Sharing and Privacy and Personal Data Protection (HLCG), but neither be restrained by the wording agreed nor be limited to the principles identified by the HLCG. The Agreement shall notably further provide:

- For definition of key terms;
- For protection of the personal data of everyone, regardless of nationality or place of residence;
- That, as regards data quality, personal data shall be processed fairly and lawfully, be accurate and, where necessary, be kept up to date;
- That, as regards purpose limitation, personal data shall be transferred and processed for specified, explicit and legitimate purposes within the scope of this agreement, i.e. preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters, and shall not be further processed in a way incompatible with those purposes;

- For the principle of data minimisation, i.e. that personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. In addition, the Agreement shall provide for an obligation to set appropriate time limits for erasure and for periodic review of the need for storage of the data;

- For the obligation for notification of any breach of personal data to the competent authority and the data subject and for a mechanism for implementing this obligation;

- That, as regards the security of processing, no person acting under the authority of the data Controller, including a processor, shall process personal data unless instructed by the Controller;

- For the logging or documentation of all processing of personal data for the sole purpose of verification of compliance with the data protection standards laid down in this Agreement;
  - For procedures enabling EU and US independent public authorities responsible for data protection to assist data subjects with exercising their rights under this Agreement, notably the right to access, rectification, erasure and redress;

  - For the right to direct access for individuals, should direct access need to be limited, the Agreement shall spell 'out the specific grounds for any necessary and proportionate restrictions. In the event of such restrictions to the right of direct access, the Agreement shall provide for indirect access by an independent public authority on behalf of the data subject;

  ~ For the right of data subjects to blocking, alongside rectification, objection and erasure;

  - For informing the data subject about the purpose of the processing, the identity of the Controller, the categories of personal data that are processed and any other information insofar as this is necessary to ensure fairness;

  - For effective and enforceable rights of administrative and judicial redress for any person whose data are processed under the Agreement;

  - That any onward transfer to and subsequent processing by competent authorities of a receiving country shall be in accordance with the rules and conditions laid down in this Agreement and any additional conditions of applicable international agreements. Moreover, the purpose limitation of the original transfer must be respected. The Agreement shall also provide that exceptions to the purpose limitation in relation to onward transfers can, in very specific circumstances for which due justification is given, be agreed upon in further specific agreements;

  - For prior written consent by the original sending country in the event of onward transfer to third countries or international organisations and for an obligation to inform, whenever possible, the data subject of any such onward transfer. In addition, the Agreement shall specify, as a condition for onward transfer, that the third country must provide an adequate level of data protection;

  - For the liability of public authorities for breaches of the Agreement, including when the data are processed on behalf of public authorities, *inter aha* laying down effective and dissuasive sanctions;

  - For the right to compensation for any person who has suffered damages as a result of unlawful processing of his or her personal data or any act incompatible with the data protection standards laid down in the Agreement.

8. The Agreement shall require that compliance with the data protection standards laid down therein shall be subject to control by one or more independent public authorities within the territory to which it applies. Each independent public authority shall have effective powers of investigation and intervention and to engage in legal proceedings or to bring to the attention of the competent judicial authorities any violations of the data protection standards in this Agreement. Each independent public authority shall, in particular, hear claims lodged by any person concerning protection of his or her rights and freedoms with regard to the processing of personal data pursuant to this Agreement. The person concerned shall be informed of the outcome of the claim.

9. The Agreement shall establish a cooperation mechanism with procedural safeguards between the independent public authorities responsible for data protection of the European Union, its Member States and the US with a view to effective Implementation of the Agreement. The parties shall mutuality ratify the designated authorities.

10. The Agreement shall stipulate that the parties shall undertake periodic joint reviews of application of the Agreement and examine how to make most effective use thereof. The joint review teams shall include representatives of public supervisory authorities of the European Union, its Member States and the US and experts from the police or the judiciary, as appropriate. The findings shah be made public.

11. The Agreement shall stipulate that its provisions shall apply to data transfers and processing concerning criminal intelligence but not to those concerning essential national security interests and specific intelligence activities in the field of national security. The Agreement shall include a narrow definition of national security interests in order not to unduly lariat the scope of the agreement.

12. The Agreement shall include a clause addressing its territorial application.

13. The Agreement shall include a clause on its duration. Whether the duration is to be indefinite or definite shall be assessed in the light of the results of negotiations. In either case, a provision shall be included requiring a review of the Agreement in due course.

14. The Agreement shall stipulate that the parties shall consult each other to facilitate resolution of any dispute regarding interpretation or application of the Agreement.

15. The Agreement shall provide for the possibilities of suspension and termination of the Agreement by either Party in the event that the above-mentioned consultation procedure is unable to resolve the dispute.

16. The Agreement shall be equally authentic in the Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish language and shall include a language clause to this effect.

17. In the course of negotiations, the Commission shall promote accession by the US to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No 108) and to its Additional Protocol with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No 181).