ROADMAP

Title of the initiative: **Recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement with the United States of America on the protection of personal data transferred for the purpose of prevention, investigation, detection or prosecution of serious criminal offences including terrorism**
Type of initiative (CWP/Catalogue/Comitology): CWP
Lead DG/contact person/details: DG JLS/A2
Expected date of adoption of the initiative (month/year): May 2010
Date of modification:
Version No: 2

Initial IA screening & planning of further work

A. Context and problem definition

(i) What is the political context of the initiative? (ii) How does this initiative relate to past and possible future initiatives, and to other EU policies?

Law enforcement agencies on both sides of the Atlantic collect and process personal data in order to prevent, detect and prosecute crime and terrorism. The transfer of personal data is 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, notably EU-Europol agreement, EU-Eurojust agreement, EU-US Mutual Legal Assistance Agreement, EU-US Passenger Name Records Agreement and the TFTP interim agreement.

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 (doc. 15851/09 JAI 822 of 23 November 2009).

The European Council of December 2009 invited the Commission in the Stockholm Programme 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. Further on the Stockholm Programme it is said that the future agreements "needs to be negotiated and concluded rapidly".

This initiative comes at a time when the Commission is also reviewing the EU data protection legal framework and preparing a strategy and legislative proposals for the protection of the fundamental right to data protection after the entry into force of the Lisbon Treaty.

What are the main problems identified?

The EU and the US share similarities but also have differences in their approaches to personal data protection. The differences create legal uncertainty for a lawful transfer of personal data for law enforcement purposes and concerns about the transfer of personal data and the rights of data subjects as recent discussions have shown.

Who is affected?

Natural and possibly legal persons residing in the European Union and in the United States of America

(i) Is EU action justified on grounds of subsidiarity? (ii) Why can the objectives of the proposed action not be achieved sufficiently by Member States (necessity test)? (iii) As a result of this, can objectives be better achieved by action by the Community (test of EU Value Added)?

Yes. Due to enhanced police and judicial cooperation between EU Member States, EU Member States hold information in their databases which originates from another EU Member State. A coherent and high level of personal data protection for the transfer of personal data to the US for the purpose of prevention, investigation, detection or prosecution of serious criminal offences including terrorism can therefore be better achieved at Union level.

B. Objectives of EU initiative

What are the main policy objectives?

The problems outlined in section A should be addressed in a legally binding EU-US agreement that ensures clarity, coherence and a high level of protection of the fundamental rights and freedoms of persons in line with the Treaty of Lisbon.

Moreover, the agreement should facilitate the negotiation of any future EU-US agreement on the transfer of specific categories of data since reference could be made to the data protection principles of the agreement in question.

Do the objectives imply developing EU policy in new areas or in areas of strategic importance?

The agreement may affect the development of the EU data protection legal framework with regard to the transfer of personal data for the purpose of prevention, investigation, detection or prosecution of serious criminal offences including terrorism.

C. Options

(i) What are the policy options? (ii) What legislative or 'soft law' instruments could be considered? (iii) Would any legislative initiatives go beyond routine up-date of existing legislation?

- No agreement but continue with specific legally binding agreements on data transfers for specific purposes
- Non-binding agreement (exchange of letters) and specific legally binding agreements on data transfer for specific purposes
- Accession of the US to the Council of Europe Convention (n°108)
- Legally binding agreement between EU and US defining data protection requirements

Does the action proposed in the options cut across several policy areas or impact on action taken/planned by other Commission departments?

The initiative touches upon several policy areas, notably external relations and may impact other policies like customs, internal market, transport and consumer rights.

Explain how the options respect the proportionality principle

The recommendation to authorise negotiation and any subsequent agreement will not go beyond what is necessary to put in place a data protection agreement for law enforcement purposes with the US. The envisaged objectives can best be achieved with a legally binding international agreement because it would provide clarity and legal certainty for both data subjects and data controllers. This approach has been endorsed by the European Council in December 2009.

D. Initial assessment of impacts

What are the significant impacts likely to result from each policy option (cf. list of impacts in the Impact Assessment Guidelines pages 32-37), even if these impacts would materialise only after subsequent Commission initiatives?

1) no agreement but continue with specific agreements on data transfers for specific purposes: legal uncertainties would persist beyond what has been achieved through specific agreements. In addition, concerns about an insufficient legal framework protecting personal data when transferred and processed in the U.S. for law enforcement purposes would continue to be voiced, notably by the European Parliament which has invited the Commission to establish such legal framework (Resolution 2008/2199 of March 2009).

2) Non-binding agreement and specific agreements on data transfers for specific purposes: legal uncertainties would persist beyond what has been achieved through specific agreements. Moreover, the differences in EU and US approaches to personal data protection which rendered the past negotiation of data protection provisions in EU US agreements regarding data transfer for law enforcement purposes particularly difficult and time-consuming would persist. There would in sum be little difference to the "no agreement" option.

3) Accession of the US to the Council of Europe Convention (n°108): This option would be desirable and generally beneficial for data transfers between the EU and the US because the Convention No 108 has been ratified by all EU Member States and provides a legally binding enumeration of data protection principles. However, the Convention allows for derogations of basic principles for data protection in the context of data processing for police, state security or crime suppression purposes which are the purposes for which we are contemplating an EU-US data protection agreement. It is our understanding that the U.S. is currently not contemplating to accede to the Council of Europe Convention No 108 which is open for accession also by non Council of Europe member states.

4) The agreement would provide legal certainty and ideally reassure data subjects in the EU that there are high data protection safeguards in place for the transfer and processing of personal data for law enforcement purposes which provide effective rights for the data subject. Such legally binding data protection framework is also considered advantageous for public authorities competent for such data transfers. A future agreement is also expected to save time and resources in case an EU-US data transfer agreement for law enforcement purposes would be envisaged in the future.

Could the options have impacts on the EU-Budget (above 5 Mio €) and/or should the IA also serve as the ex-ante evaluation, required by the Financial Regulation?

No

Could the options have significant impacts on (i) simplification, (ii) administrative burden or on (iii) relations with third countries?

The options would impact on relations with the U.S., possibly also with other countries.

E. Planning of further impact assessment work

When will the impact assessment work start?

No impact assessment is planned.

(i) What information and data are already available? (ii) Will this impact assessment build on already existing impact assessment work or evaluations carried out? (iii) What further information needs to be gathered? (iv) How will this be done (e.g. internally or by an external contractor) and by when?
(v) What type and level of analysis will be carried out (cf. principle of proportionate analysis)?

N/A

Which stakeholders & experts have been/will be consulted, how and at what stage?

A public consultation via the "your voice in Europe" website was online from 28 January to 12 March 2010. Three stakeholder meetings were organised with data protection experts, private sector representatives and police representatives and EU Member States representatives, respectively on 2 February, 26 February and 10 March 2010.