COUNCIL OF THE EUROPEAN UNION

Brussels, 3 February 2012

5999/12

LIMITE

JAI 53
USA 2
DATAPROTECT 13
RELEX 76

NOTE

from:	Commission services
to:	JHA Counsellors
No. prev. doc.:	17480/10 JAI 1049 USA 127 DATAPROTECT 98 RELEX 1069 RESTREINT UE
Subject:	EU-US data protection negotiations during 2011

Delegations find in Annex a note from the Commission DG JUSTICE on EU-US data protection negotiations during 2011.

On 3 December 2010, the Council adopted a decision authorising the Commission to open negotiations on 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.

On 28 March 2011 the Commission opened negotiations with the US side. Further negotiation sessions were held on 5-6 May, 26 May, 24 June, 28 July, 9 September, 9 November and 13 December 2011. In addition, at technical level meetings were held on 17 May and 18 July 2011. The next negotiation session is scheduled for 13 February 2012. A technical expert seminar on protection of personal data exchanged in the framework of police cooperation and judicial cooperation in criminal matters is also envisaged.

In accordance with Article 2 of the Council decision authorising the opening of negotiations, the Commission has reported after each negotiating session to the designated special committee (JHA Counsellors) on the progress of the negotiations.

In accordance with Article 218(8) TFEU, the European Parliament has likewise been immediately and fully informed, in the framework of its Committee for Civil Liberties, Justice and Home Affairs.

One year since the adoption of the negotiating directives by the Council, the Commission services consider it appropriate to provide a written overview of the issues addressed in the negotiations to date. The enclosed non-paper serves this purpose. It will also be shared with the European Parliament for information. The paper is marked 'LIMITE' and should be afforded appropriate handling.

EU-US DATA PROTECTION NEGOTIATIONS
NON-PAPER ON NEGOTIATIONS DURING 2011

Since the start of negotiations, a detailed first exchange of views has been held on all the issues covered by the Commission's negotiating directives. This has included detailed explanations on how respective domestic legal systems work, how specific legal concepts are to be understood, based on domestic legislation and jurisprudence.

Regarding the **purpose** of the agreement, both sides agree that the agreement itself will not be the legal basis for any transfers of personal data and that a specific legal basis for such transfers will always be required. The US wishes to achieve mutual recognition of the respective data protection systems ("adequacy"). Furthermore, the US side has a mandate for an "Executive agreement" that does not change existing US law, nor create any new rights. The US therefore aims to limit the agreement to integrating principles from existing EU-US agreements (Eurojust, MLA, Europol agreements) and the EU-US High Level Contact Group (HLCG). Further discussions are needed to achieve all objectives of the negotiating directives.

Regarding the **scope** of application of the agreement, the possible application to existing bilateral data-sharing agreements concluded by Member States has been postponed for a later stage, as this can only be meaningfully done after the content of the agreement has become clearer.

On the **material scope of the agreement**, the US side proposed to differentiate between "case-specific" (exchange of personal information between police and judicial authorities in the framework of an investigation) and "program-based" (large-scale data transfers such as PNR, TFTP) information. The US has rejected the idea to apply the agreement also to data transferred from private parties in the EU to private parties in the US and subsequently processed for law enforcement purposes by US competent authorities. Both sides agree in substance that the agreement should be without prejudice to the activities in the field of national security, which remains the sole responsibility of Member States.

Further discussions are needed to achieve all objectives as regards the scope of the agreement.

Regarding **data subjects' rights,** the US side envisages an "Executive agreement" that cannot create any individual rights (see above). The Commission's negotiating directives are clear on the content and enforcement of data subjects' rights. In this context also a **non-discrimination clause**, i.e. the application of data protection principles to all data subjects regardless of nationality and place of residence, was discussed. The US is cautious on this as it is linked to the personal scope of protection under the Privacy Act, which is limited to US citizens and permanent residents.

As regards the content of the rights:

On the right to information of data subjects, the US side defended its existing system of general notice and opposed the idea of changing its legislation in order to provide for information of data subjects in the law enforcement context.

Right to access by data subject, the US side argued that access rights are adequately guaranteed in the US in particular by the Freedom of Information Act (FOIA). Further discussion will be needed on the definition of and extent of law enforcement exemptions to the right to access.

On the rights to rectification, erasure and blocking, the US expressed fears that, as a result of data subjects' requests, erasure or rectification would have to be granted during a trial or investigation (e.g. allowing suspects to erase their own statements). This reflects a misconception of the actual application of the rights to rectification and erasure, which has to be further clarified in order to allow for progress.

On automated decision-making, both sides have a general understanding based on the relevant HLCG principle. Further work is needed to formulate a provision in this respect.

On redress, the US side argues that the US system offers equally effective protection in practice. The US side refers in particular to judicial redress regarding access requests under FOIA and to judicial redress, including compensation (on the basis of tort law), where data subjects have suffered damages. The US side thus proposes to refer in the Agreement to the availability of judicial redress and compensation for data subjects who have suffered damages, in accordance with the existing US laws and list them in the agreement (Computer Fraud and Abuse Act, Federal Tort Claims Act, The Electronic Communications Privacy Act, Mandatory Victims Restitution Act). The US side however acknowledged that no judicial redress is available to non-US individuals who seek correction of their data without having suffered harm. Further discussion is needed.

Discussions progressed slightly on administrative redress mechanisms. The US side proposed that individuals can either seek administrative redress as provided for by the other party's domestic law or ask their Data Protection Authority (DPA) or Chief Privacy Officer to refer a matter to the competent authority of the other party on their behalf.

As regards compensation for data subjects who have suffered damages as a result of unlawful processing of their data or any act incompatible with the provisions of the Agreement, the US side referred that an Executive agreement under US law cannot create any individual rights, including rights to compensation. More information on what type of compensation is currently available to data subjects under US law has been requested.

Further discussions to achieve all objectives identified in the negotiating directives are required, this concerns the content and the form of data subjects rights, in particular for judicial redress.

Regarding **data retention**, the US side appears to oppose a general obligation enshrined in this agreement to define appropriate retention periods whenever data sharing is agreed (specific agreements, unilateral condition by sending authority), arguing that such limits should be determined by the recipient party's domestic law. The US has accepted that retention periods for "programme-based" exchange of data should not be left to the recipient party's domestic law. Further discussions are needed to achieve all objectives of the negotiating directives.

As regards **onward transfers**, some progress was made by agreeing on a principle that, for "case-specific" data sharing, the sending authority's prior consent is a precondition for any onward transfer of data to a third country. As regards "programme-based" data onward sharing, this element requires further discussion.

On **purpose limitation (and further use of data)**, the US envisages to specify the purpose of data processing and further use in the "umbrella" agreement itself and to conceive it widely. This would result that in principle all data could be used for prevention, detection, suppression, investigation or prosecution of criminal offences, protection of public security, for directly related non-criminal and administrative proceedings, or for any other purpose if prior consent is given by the sending authority. Further discussions are needed to achieve all objectives of the negotiating directives.

Progress was made on **data security**, as both sides broadly agreed on the importance of processing personal data in a secure way and restricting access to authorised persons, using relevant technological safeguards. Further work is needed to formulate a provision in this respect.

On **data breach notification**, both sides agreed on the notion in principle. The Commission argued that the recipient authority should notify data breaches to the sending authority and, unless certain exemptions for law enforcement interests apply, also to the data subject. After the US side argued that only *serious* breaches should be notified, it was provisionally agreed that all *significant* breaches should be notified to the sending authority and data subject (although certain exemptions should apply for the latter).

On **logging** of data processing, both sides agreed in principle and further work is needed on formulating a provision to reflect the objectives of the negotiating directives.

As regards **sensitive data**, there is a general understanding that such data should only be processed in restricted cases and with appropriate safeguards, like in the HLCG principle. However further work is needed to formulate a provision in this respect.

Regarding **lawfulness and proportionality**, the US side appears reluctant to transpose this HLCG principle in the agreement, arguing that the term "proportionality" is not in US law and therefore its effect is unknown. Discussions will be continued.

As regards **liability** of public officials, the US side explained that according to the existing US law officials can be prosecuted for serious misconduct, including inappropriate use of personal data, but no specific regime of sanctions for violation of data protection rules exists. Further discussions are needed to achieve objectives of the negotiating directives.

Regarding **oversight**, the US side argued that its existing institutions (like Chief Privacy Officers, Inspectors General, Government Accountability Office) overall ensure effective oversight over the processing of personal data by federal government agencies. In order to strengthen oversight specifically on privacy and data protection issues, the Commission suggested giving the US Privacy and Civil Liberties Oversight Board (PCLOB) a role in ensuring independent oversight over data protection matters covered by the agreement. Further discussions are needed to achieve all objectives of the negotiating directives.

Regarding **joint reviews** of the future Agreement, the US wishes to avoid a burdensome or expensive process. Discussions will be continued.

_____