Council of the European Union
General Secretariat

Brussels, 16 March 2015
(OR. en)

7236/15

RESTREINT UE/EU RESTRICTED

JAI 177
USA 10
DATAPROTECT 32
RELEX 228

NOTE

From:	Commission Services
To:	Delegations
Subject:	Agreement between the European Union and the United States of America on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism

Delegations will find in the Annex, the Commission Services draft text for the provisions of the above agreement that have been agreed so far.

DRAFT AGREEMENT

between the European Union and the United States of America on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism

Article 1 : Purpose of the Agreement

1. The purpose of this Agreement is to ensure a high level of protection of personal information and enhance cooperation between the United States, European Union and its Member States, in relation to the prevention, investigation, detection or prosecution of criminal offenses, including terrorism.

2. For this purpose, this Agreement establishes the framework for the protection of personal information when transferred between the [Parties].

3. This Agreement in and of itself shall not be the legal basis for any transfers of personal information. A legal basis for such transfers shall always be required.

Article 4: Scope

1. This Agreement shall apply to personal information transferred between the Competent Authorities of [the Parties] or otherwise transferred in accordance with an agreement concluded between the United States and the European Union or its Member States, for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

2. This Agreement does not affect, and is without prejudice to, transfers or other forms of cooperation between the competent authorities of the Member States and the United States responsible for safeguarding national security.

Article 5: Non-Discrimination

[This article is still under discussion with the US]

Article 6: Effect of the Agreement

1. This Agreement supplements, as appropriate, but does not replace, provisions regarding the protection of personal information in international agreements between the Parties, or between the US and Member States, that address matters within the scope of this Agreement.

2. The Parties shall take all necessary measures to implement this Agreement, including, in particular, their respective obligations regarding access, rectification and administrative and judicial redress for individuals provided herein. The protections and remedies set forth in this Agreement shall benefit individuals and entities in the manner implemented in the applicable domestic laws of each Party.

3. By giving effect to paragraph 2, the processing and use of personal information by the US, or the EU and its Member States, with respect to matters falling within the scope of this Agreement, shall be deemed to comply with their respective data protection legislation restricting or conditioning international transfers of personal information, and no further authorization under such legislation shall be required.

Article 7: Purpose and use limitations

1. The transfer of personal information shall be for specific purposes authorised by the legal basis for the transfer as set forth in Article 1.

2. The further processing or use of personal information by a Party shall not be incompatible with the purposes for which it was transferred. Compatible processing or use includes processing or use pursuant to the terms of existing international agreements and written international frameworks for the prevention, detection, investigation or prosecution of serious crimes. All such processing and use of personal information shall be subject to the other provisions of this Agreement.

3. This Article shall not prejudice the ability of the transferring Competent Authority to impose additional conditions in a specific case to the extent the applicable legal framework for transfer permits it to do so. Such conditions shall not include generic data protection conditions, that is, conditions imposed that are unrelated to the specific facts of the case. If the information is subject to conditions, the receiving Competent Authority shall comply with them. The Competent Authority providing the information may also require the recipient to give information on the use made of the transferred information.

4. Where the [Parties] conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, the specified purposes for which the information is transferred and processed or used shall be set forth in that agreement.

5. The Parties shall ensure under their respective laws that personal information is processed or used in a manner that is directly relevant to and not excessive or overbroad in relation to the purposes of such processing or use.

Article 8: Onward transfer

1. Where the [Parties] have transferred personal information relating to a specific case, that information may be transferred to a third State or international body only where the prior consent of the Competent Authority originally transferring that information has been obtained.

2. When granting its consent to a transfer under paragraph 1, the Competent Authority originally transferring the information shall take due account of all relevant factors, including the seriousness of the offence, the purpose for which the data is initially transferred and whether the third State or international body in question ensures an appropriate level of protection of personal information. It may also subject the transfer to specific conditions.

3. Where the [Parties] conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, the onward transfer of personal information to a third State or international body may only take place in accordance with specific conditions set forth in the agreement that provide due justification for the onward transfer. The agreement shall also provide for appropriate information mechanisms between the Competent Authorities.

Article 9: Maintaining Quality and Integrity of Information

The Parties shall take reasonable steps to ensure that personal information is maintained with such accuracy, relevance, timeliness and completeness as is necessary and appropriate for lawful processing of the information. For this purpose, the Parties shall have in place procedures, the object of which is to ensure the quality and integrity of personal information, including the following:

(a) the measures referred to in Article 18;

(b) where the transferring [Competent] Authority becomes aware of significant doubts as to the relevance, timeliness, completeness or accuracy of such personal information or an assessment it has transferred, it shall, where feasible, advise the receiving [Competent] Authority thereof;

(c) where the receiving [Competent] Authority becomes aware of significant doubts as to the relevance, timeliness, completeness or accuracy of personal information received from a governmental authority, or of an assessment made by the transferring [Competent] Authority of the accuracy of information or the reliability of a source, it shall, where feasible, advise the transferring [Competent] Authority thereof.

Article 10: Information Security

The Parties shall ensure that they have in place appropriate technical, security and organizational arrangements for the protection of personal information against all of the following:

(a) accidental or unlawful destruction;

(b) accidental loss; and

(c) unauthorized disclosure, alteration, access, or other processing or use.

Such arrangements shall include appropriate safeguards regarding the authorization required to access personal information.

Article 11 : Notification of an information security incident

1. Upon discovery of an incident involving accidental loss or destruction, or unauthorized access, disclosure, or alteration of personal information, in which there is a significant risk of damage, the [recipient] [receiving Competent Authority] shall promptly assess the likelihood and scale of damage to individuals and to the integrity of the [provider's] [transferring Competent Authority's] program, and promptly take appropriate action to mitigate any such damage.

2. Action to mitigate damage shall include notification to the [provider] [transferring Competent] Authority's. However, notification may:

(a) include appropriate restrictions as to the further transmission of the notification;

(b) be delayed or omitted when such notification may endanger national security;

(c) be delayed when such notification may endanger public security operations.

3. Action to mitigate damage shall also include notification to the individual, where appropriate given the circumstances of the incident, unless such notification may endanger:

(a) public or national security;

(b) official inquiries, investigations or proceedings;

(c) the prevention, detection, investigation, or prosecution of criminal offenses;

(d) rights and freedoms of others, in particular the protection of victims and witnesses.

4. The Competent Authorities involved in the transfer of the personal information may consult concerning the incident and the response thereto.

Article 12: Maintaining Records

1. The Parties shall have in place effective methods of demonstrating the lawfulness of processing and use of personal information, which may include the use of logs, as well as other forms of records.

2. The Competent Authorities may use such logs or records for maintaining orderly operations of the databases or files concerned, to ensure data integrity and security, and where necessary to follow backup procedures.

Article 13: Retention Period

1. The Parties shall provide, in their applicable legal frameworks, specific retention periods for records containing personal information, the object of which is to ensure that personal information is not retained for longer than is necessary and appropriate. Such retention periods shall take into account the purposes of processing or use, the nature of the data and the authority processing it, the impact on the relevant rights and interests of affected persons, and other applicable legal considerations.

2. Where the [Parties] conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, such agreement will include a specific and mutually agreed upon provision on retention periods.

3. The Parties-shall provide procedures for periodic review of the retention period with a view to determining whether changed circumstances require further modification of the applicable period.

4. The Parties shall publish or otherwise make publicly available such retention periods.

Article 14: Special categories of Personal Information

1. Processing or use of personal information revealing racial or ethnic origin, political opinions or religious or other beliefs, trade union membership or personal information concerning health or sexual life shall only take place under appropriate safeguards in accordance with law. Such appropriate safeguards may include: restricting the purposes for which the information may be processed or used, such as allowing the processing or use only on a case by case basis; masking, deleting or blocking the information after effecting the purpose for which it was processed or used; restricting personnel permitted to access the information; requiring specialized training to personnel who access the information; requiring supervisory approval to access the information; or other protective measures. These safeguards shall duly take into account the nature of the information, particular sensitivities of the information, and the purpose for which the information is processed or used.

2. Where the [Parties] conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, such an agreement will further specify the standard and conditions under which such information can be processed, duly taking into account the nature of the information and the purpose for which it is used.

Article 15: Accountability

The Parties shall have in place measures to promote accountability by their authorities in carrying out this Agreement in accordance with their respective laws. Serious misconduct shall be addressed through appropriate and dissuasive criminal, civil or administrative sanctions.

Article 16: Automated Decisions

Decisions producing significant adverse actions concerning the relevant interests of the individual may not be based solely on the automated processing of personal information without human involvement, unless authorized under domestic law, and with appropriate safeguards that include the possibility to obtain human intervention.

Article 17: Access

1. The Parties shall ensure that any individual is entitled to seek access to his or her personal information and, subject to the restrictions set forth in paragraph 2, to obtain it. Such access shall be sought and obtained in accordance with the applicable legal framework of the State in which relief is sought.

2. The obtaining of such personal information in a particular case may be subject to reasonable restrictions provided under domestic law, taking into account legitimate interests of the individual concerned, so as to:

a. protect the rights and freedoms of others, including their privacy;

b. safeguard public and national security;

c. protect law enforcement sensitive information;

d. avoid obstructing official or legal inquiries, investigations or proceedings;

e. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties;

f. otherwise protect interests provided for in legislation regarding freedom of information and public access to documents.

3. Excessive expenses shall not be imposed on the individual as a condition to access his or her personal information.

4. An individual is entitled to authorize, where permitted under applicable domestic law, an oversight authority or other representative to request access on his or her behalf.

5. If access is denied or restricted, the requested Competent Authority will, without undue delay, provide to the individual, or to his or her duly authorized representative as set forth in paragraph 4, the reasons for the denial or restriction of access.

Article 18: Rectification

1. The Parties shall ensure that any individual is entitled to seek correction or rectification of his or her personal information that he or she asserts is either inaccurate or has been improperly processed. Correction or rectification may include supplementation, erasure, blocking or other measures or methods. Such correction or rectification shall be sought and obtained in accordance with the applicable legal framework of the State in which relief is sought.

2. Where the receiving Competent Authority concludes following:

a. a request under paragraph 1 ;

b. notification by the provider; or

c. its own investigations or inquiries;

that the information it has received under this Agreement is inaccurate or has been improperly processed, it shall take measures of supplementation, erasure, blocking or other methods of correction or rectification, as appropriate.

3. An individual is entitled to authorize, where permitted under applicable domestic law, an oversight authority or other representative to seek correction or rectification on his or her behalf.

4. If correction or rectification is denied or restricted, the requested Competent Authority will, without undue delay, provide to the individual or to his or to her duly authorized representative as set forth in paragraph 3, a response setting forth the basis for the denial or restriction of correction or rectification.

Article 19: Administrative Redress

1. The Parties shall ensure that any individual is entitled to seek administrative redress where he or she believes that his or her request pursuant to Articles [17] or [18] was improperly denied, or his or her personal information was otherwise improperly processed or used. Such redress shall be sought and obtained in accordance with the applicable legal framework of the State in which relief is sought.

2. An individual is entitled to authorize, where permitted under applicable domestic law, an oversight authority or other representative to seek administrative redress on his or her behalf.

3. The Competent Authority from which relief is sought shall carry out the appropriate inquiries and verifications and without undue delay shall respond in written form, including through electronic means, with the result, including, the ameliorative or corrective action taken where applicable. Notice of the procedure for seeking any further administrative redress shall be as provided for in Article 21.

Article 21: Transparency

1. The Parties shall provide notice to an individual, as to his or her personal information, which notice may be effected by the Competent Authority through publication of general notices or through actual notice, in a form and at a time provided for by the law applicable to the authority providing notice, with regard to the:

(a) purposes of processing or use of such information by that authority;

(b) purposes for which the information may be shared with other Competent Authorities;

(c) laws or rules under which such processing or use takes place;

(d) third parties to whom such information is disclosed; and

(e) access, correction or rectification, and redress available.

2. Such notice requirement is subject to the reasonable restrictions under domestic law with respect to the matters set forth in Article [17 (2) (a) through [(i)].

Article 22: Effective Oversight

1. The Parties shall have in place one or more public oversight authorities that:

(a) exercise independent oversight functions and powers, including review, investigation and intervention, where appropriate on their own initiative;

(b) have the power to accept and act upon complaints made by individuals relating to the measures implementing this Agreement; and

(c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action when appropriate.

2. The European Union shall provide for oversight under this Article through its data protection authorities and those of its Member States.

3. The United States shall provide for oversight under this Article cumulatively through more than one authority, which may include, inter alia, inspectors general, chief privacy officers, government accountability offices, privacy and civil liberties oversight boards, and other applicable executive and legislative privacy or civil liberties review bodies.1

Article 23: Cooperation between oversight authorities

1. Consultations between authorities conducting oversight under Article [22] shall take place as appropriate with respect to carrying out the functions in relation to this Agreement, with a view towards ensuring effective implementation of the provisions of Articles [17], [18] and [19].

2. The Parties shall establish national contact points which will assist with the identification of the oversight authority to be addressed in a particular case.

Article 24: Joint Review

1. The Parties shall conduct periodic joint reviews of the policies and procedures that implement this Agreement and of their effectiveness. Particular attention in the joint reviews shall be paid to the effective implementation of the protections under Article [17] on access, Article [18] on rectification, Article [19] on administrative redress, and Article [20] on judicial redress.

2. The first joint review shall be conducted no later than three years from the date of entry into force of this Agreement and thereafter on a regular basis. The Parties shall jointly determine in advance the modalities and terms thereof and shall communicate to each other the composition of their delegations, which shall include representatives of the public oversight authorities referred to in Article [22] on effective oversight, and of law enforcement and justice authorities. The findings of the joint reviews will be made public.

3. Where the Parties or the United States and a Member State have concluded another agreement, the subject matter of which is also within the scope of this Agreement, which provides for joint reviews, such joint reviews shall not be duplicated and, to the extent relevant, their findings shall be made part of the findings of the joint review of this Agreement.

Article 25: Notification

1. The United States shall notify the European Union of any designation made by United States authorities in relation to Article 20, and any modifications thereto.

2. The Parties shall make reasonable efforts to notify each other regarding the enactment of any laws or adoption of regulations that materially affect the implementation of this Agreement, where feasible before they become effective.

Article 26: Consultation

Any dispute arising from the interpretation or application of this Agreement shall give rise to consultations between the Parties with a view to reaching a mutually agreeable resolution.

Article 28: Territorial application

1. This Agreement will only apply to Denmark, the United Kingdom, or Ireland if the European Commission notifies the United States in writing that Denmark, the United Kingdom, or Ireland has decided that this Agreement will apply to its State.

2. If the European Commission notifies the United States before the entry into force of this Agreement that this Agreement will apply to Denmark, the United Kingdom, or Ireland, this Agreement shall apply to such States from the date of entry into force of the Agreement.

3. If the European Commission notifies the United States after the entry into force of this Agreement that it applies to Denmark, the United Kingdom, or Ireland, this Agreement shall apply to such State on the first day of month following receipt of the notification by the United States.

Article 29: Duration of the Agreement

This Agreement is concluded for an unlimited duration.

Article 30: Entry into force and Termination

1. This Agreement shall enter into force on the first day of the month following the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for entry into force.

2. Either Party may terminate this Agreement by written notification to the other Party through diplomatic channels. Such termination shall take effect thirty days from the date of receipt of such notification.

3. Notwithstanding any termination of this Agreement, personal information falling within the scope of this Agreement and transferred prior to its termination shall continue to be processed in accordance with this Agreement.

IN WITNESS WHEREOF, the undersigned Plenipotentiaries have signed this Agreement.