



Council of the
European Union

Brussels, 31 October 2019
(OR. en)

8761/14
ADD 1 DCL 1

JAI 220
USA 9
DATAPROTECT 56
RELEX 319

DECLASSIFICATION

of document: 8761/14 ADD 1 RESTREINT UE/EU RESTRICTED
dated: 16 April 2014
new status: Public

Subject: EU-US data protection "Umbrella Agreement"
- Draft text of the provisions agreed so far

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 16 April 2014

**8761/14
ADD 1**

RESTREINT UE/EU RESTRICTED

**JAI 220
USA 9
DATAPROTECT 56
RELEX 319**

NOTE

from : Commission Services

to : JHA Counsellors

No. prev. doc. : 8761/14 JAI 220 USA 9 DATAPROTECT 56 RELEX 319
5999/12 JAI 53 USA 2 DATAPROTECT 13 RELEX 76
17480/10 JAI 1049 USA 127 DATAPROTECT 98 RELEX 1069
RESTREINT UE

Subject : EU-US data protection "Umbrella Agreement"
- Draft text of the provisions agreed so far

Delegations will find in Annex the draft text of the provisions agreed so far on the EU-US data protection "Umbrella Agreement".

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

[draft text of the provisions agreed so far]

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 3: 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 [Parties], 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 of the European Union and the United States responsible for safeguarding national security.

Article 4: Non-Discrimination

Each Party shall apply the provisions of this Agreement without discrimination between its own nationals and residents and those of the other Party.

Article 8: Maintaining Quality and Integrity of Information

The [United States, the European Union, and its Member States, respectively,] [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 [United States, the European Union, and its Member States, respectively,] [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 [EU 12/US 8];
- (b) where the provider 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 recipient thereof;
- (c) where the recipient 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 provider of the accuracy of information or the reliability of a source, it shall, where feasible, advise the provider thereof.

Article 10: 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 [US: program-based information] / [EU: personal information not relating to a specific case], such agreement will include a specific and mutually agreed upon provision on retention period.
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 periods¹.

Article 11: Maintaining Records

1. The [United States, the European Union, and its Member States, respectively,] [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 authority 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 12: Data Security

The [United States, the European Union, and its Member States, respectively,] [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

¹ EU reserves the possible reference to the need to jointly review the implementation of retention periods, in accordance with the Article on joint reviews.

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

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

Article 13: 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 shall promptly assess the likelihood and scale of damage to individuals and to the integrity of the provider's program, and promptly take appropriate action to mitigate any such damage.

2. Action to mitigate damage shall include notification to the provider. 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 authorities involved in the transfer of the personal information may consult concerning the incident and the response thereto.

Article 15: 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 sending that information has been obtained.
2. When granting its consent to a transfer under paragraph 1, the competent authority originally sending 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 to transfer personal information [U.S.: relating to program based information][EU: not relating to a specific case,] 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 18: 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 19: Transparency

1. The [United States, the European Union, and its Member States, respectively,] [Parties] shall provide notice to an individual, as to his or her personal information, which notice may be effected 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 [EU 20/US 15 (2) (a) through [(f)].

Article 20: Access

1. The [United States, the European Union, and its Member States, respectively,] [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 person 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 procedures;

- e. avoid prejudicing the prevention, detection, investigation and 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 authority will, without undue delay, provide to the individual, or his or her duly authorized representative as set forth in paragraph 4, the reasons for the denial or restriction of access.

Article 21: 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 competent authority of the recipient 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 authority will, without undue delay, provide to the individual or his or 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 22: Administrative Redress

1. The [United States, the European Union, and its Member States, respectively,] [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 [EU 20/US 15 or EU 21/US 16] was improperly denied, or his or her personal information was otherwise improperly processed. 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 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 19.

Article 24: Accountability

The [United States, the European Union, and its Member States, respectively,] [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 25: Effective Oversight

1. The [United States, the European Union, and its Member States, respectively] [Parties] shall have in place one or more public oversight authorities which:

(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 and its Member States, respectively, shall provide for oversight under this Article through their data protection authorities.

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.

Article 26: Cooperation between oversight authorities

1. Consultations between authorities conducting oversight under Article [EU 25/US 19] 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 [EU 20/US 15], [EU 21/US 16] and [EU 22/US 17].

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.