EUROPEAN
COMMISSION

Brussels, 29.4.2016
COM(2016) 237 final

ANNEX 1

**ANNEX**

# AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION ON THE PROTECTION OF PERSONAL INFORMATION RELATING TO THE PREVENTION, INVESTIGATION, DETECTION, AND PROSECUTION OF CRIMINAL OFFENSES

***accompanying***

**Proposal for a Council Decision**

**on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses**

**AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION ON THE PROTECTION OF PERSONAL INFORMATION RELATING TO THE PREVENTION, INVESTIGATION, DETECTION, AND PROSECUTION OF CRIMINAL OFFENSES**

**TABLE OF CONTENTS**


Preamble

Article 1: Purpose

Article 2: Definitions

Article 3: Scope

Article 4: Non-discrimination

Article 5: Effect of the Agreement

Article 6: Purpose and Use Limitations

Article 7: Onward Transfer

Article 8: Maintaining the Quality and Integrity of Information

Article 9: Information Security

Article 10: Notification of an Information Security Incident

Article 11: Maintaining Records

Article 12: Retention Period

Article 13: Special Categories of Personal Information

Article 14: Accountability

Article 15: Automated Decisions

Article 16: Access

Article 17: Rectification

Article 18: Administrative Redress

Article 19: Judicial Redress

Article 20: Transparency

Article 21: Effective Oversight

Article 22: Cooperation between Oversight Authorities

Article 23: Joint Review

Article 24: Notification

Article 25: Consultation

Article 26 : Suspension

Article 27: Territorial Application

Article 28: Duration

Article 29: Entry into force and Termination

*Mindful* that the United States and the European Union are committed to ensuring a high level of protection of personal information exchanged in the context of the prevention, investigation, detection, and prosecution of criminal offenses, including terrorism;

*Intending* to establish a lasting legal framework to facilitate the exchange of information, which is critical to prevent, investigate, detect and prosecute criminal offenses, including terrorism, as a means of protecting their respective democratic societies and common values;

*Intending*, in particular, to provide standards of protection for exchanges of personal information on the basis of both existing and future agreements between the US and the EU and its Member States, in the field of preventing, investigating, detecting, and prosecuting criminal offenses, including terrorism;

*Recognizing* that certain existing agreements between the Parties concerning the processing of personal information establish that those agreements provide an adequate level of data protection within the scope of those agreements, the Parties affirm that this Agreement should not be construed to alter, condition, or otherwise derogate from those agreements; noting however, that the obligations established by Article 19 of this Agreement on judicial redress would apply with respect to all transfers that fall within the scope of this Agreement, and that this is without prejudice to any future review or modification of such agreements pursuant to their terms;

*Acknowledging* both Parties' longstanding traditions of respect for individual privacy including as reflected in the Principles on Privacy and Personal Data Protection for Law Enforcement Purposes elaborated by the EU-U.S. High Level Contact Group on Information Sharing and Privacy and Personal Data Protection, the Charter of Fundamental Rights of the European Union and applicable EU laws, the United States Constitution and applicable U.S. laws, and the Fair Information Practice Principles of the Organization for Economic Cooperation and Development; and

*Recognizing* the principles of proportionality and necessity, and relevance and reasonableness, as implemented by the Parties in their respective legal frameworks;

THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION HAVE AGREED AS FOLLOWS:

**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 and the 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 United States, on the one hand, and the European Union or its Member States, on the other.

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 2: Definitions**

For purposes of this Agreement:

1. "Personal information" means information relating to an identified or identifiable natural person. An identifiable person is a person who can be identified, directly or indirectly, by reference to, in particular, an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

2. "Processing of personal information" means any operation or set of operations involving collection, maintenance, use, alteration, organization or structuring, disclosure or dissemination, or disposition.

3. "Parties" means the European Union and the United States of America.

4. "Member State" means a Member State of the European Union.

5. "Competent Authority" means, for the United States, a U.S. national law enforcement authority responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism and, for the European Union, an authority of the European Union, and an authority of a Member State, responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism.

**Article 3: Scope**

1. This Agreement shall apply to personal information transferred between the Competent Authorities of one Party and the Competent Authorities of the other Party, 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 authorities of the Member States and of the United States other than those referred to in Article 2(5), responsible for safeguarding national security.

**Article 4: Non-Discrimination**

Each Party shall comply with its obligations under this Agreement for the purpose of protecting personal information of its own nationals and the other Party's nationals regardless of their nationality, and without arbitrary and unjustifiable discrimination.

**Article 5: 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 the United States 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. For the United States, its obligations shall apply in a manner consistent with its fundamental principles of federalism.

3. By giving effect to paragraph 2, the processing of personal information by the United States, or the European Union 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 6: Purpose and Use Limitations**

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

2. The further processing of personal information by a Party shall not be incompatible with the purposes for which it was transferred. Compatible processing includes processing 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 of personal information by other national law enforcement, regulatory or administrative authorities shall respect 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 United States, on the one hand, and the European Union or a Member State on the other, 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 shall be further set forth in that agreement.

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

**Article 7: Onward Transfer**

1. Where a Competent Authority of one Party has transferred personal information relating to a specific case to a Competent Authority of the other Party, that information may be transferred to a State not bound by the present Agreement 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 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 State not bound by the present Agreement 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 United States, on the one hand, and the European Union or a Member State on the other, 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 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.

4. Nothing in this Article shall be construed as affecting any requirement, obligation or practice pursuant to which the prior consent of the Competent Authority originally transferring the information must be obtained before the information is further transferred to a State or body bound by this Agreement, provided that the level of data protection in such State or body shall not be the basis for denying consent for, or imposing conditions on, such transfers.

**Article 8: 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 Competent Authorities 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 17;

(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 9: 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.

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

**Article 10: 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 receiving Competent Authority shall promptly assess the likelihood and scale of damage to individuals and to the integrity of the 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 transferring Competent Authority. 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 11: Maintaining Records**

1. The Parties shall have in place effective methods of demonstrating the lawfulness of processing 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 12: 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, the nature of the data and the authority processing it, the impact on relevant rights and interests of affected persons, and other applicable legal considerations.

2. Where the United States, on the one hand, and the European Union or a Member State on the other, 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 13: Special Categories of Personal Information**

1. Processing 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, such as allowing the processing only on a case by case basis; masking, deleting or blocking the information after effecting the purpose for which it was processed; 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.

2. Where the United States, on the one hand, and the European Union or a Member State on the other, conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, such agreement will further specify the standards 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 14: Accountability**

1. The Parties shall have in place measures to promote accountability for processing personal information within the scope of this Agreement by their Competent Authorities, and any other

of their authorities to which personal information has been transferred. Such measures shall include notification of the safeguards applicable to transfers of personal information under this Agreement, and of the conditions that may have been imposed by the transferring Competent Authority pursuant to Article 6(3). Serious misconduct shall be addressed through appropriate and dissuasive criminal, civil or administrative sanctions.

2. The measures set out in paragraph 1 shall include, as appropriate, discontinuation of transfer of personal information to authorities of constituent territorial entities of the Parties not covered by this Agreement that have not effectively protected personal information, taking into account the purpose of this Agreement, and in particular the purpose and use limitations and onward transfer provisions of this Agreement.

3. In case of allegations of improper implementation of this Article, a Party may request the other Party to provide relevant information, including, where appropriate, regarding the measures taken under this Article.

**Article 15: 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 16: 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 from a Competent Authority in accordance with the applicable legal framework of the State in which relief is sought.

2. The obtaining of such 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 17: 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 for addressing inaccuracies or improper processing. Such correction or rectification shall be sought and obtained from a Competent Authority 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 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 18: 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 for access pursuant to Article 16 or rectification of inaccurate information or improper processing pursuant to Article 17 has been improperly denied. Such redress shall be sought and obtained from a Competent Authority 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 20.

**Article 19: Judicial Redress**

1. The Parties shall provide in their applicable legal frameworks that, subject to any requirements that administrative redress first be exhausted, any citizen of a Party is entitled to seek judicial review with regard to:

a) denial by a Competent Authority of access to records containing his or her personal information;

b) denial by a Competent Authority of amendment of records containing his or her personal information; and

c) unlawful disclosure of such information that has been willfully or intentionally made, which shall include the possibility of compensatory damages.

2. Such judicial review shall be sought and obtained in accordance with the applicable legal framework of the State in which relief is sought.

3. Paragraphs 1 and 2 are without prejudice to any other judicial review available with respect to the processing of an individual's personal information under the law of the State in which relief is requested.

4. In the event of the suspension or termination of the Agreement, articles 26(2) or 29(3) shall not create a basis for judicial redress that is no longer available under the law of the Party concerned.

**Article 20: 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 Authorities 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 of such information by that authority;

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

(c) laws or rules under which such processing 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 16(2) (a) through (f).

**Article 21: 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 the 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.

**Article 22: Cooperation between oversight authorities**

1. Consultations between authorities conducting oversight under Article 21 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 16, 17, and 18.

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

**Article 23: 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 14 on accountability, Article 16 on access, Article 17 on rectification, Article 18 on administrative redress, and Article 19 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 respective delegations, which shall include representatives of the public oversight authorities referred to in Article 21 on effective oversight, and of law enforcement and justice authorities. The findings of the joint review 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 24: Notification**

1. The United States shall notify the European Union of any designation made by U.S. authorities in relation to Article 19, and any modifications thereto.

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

**Article 25: 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 26: Suspension**

1. In the event of a material breach of this Agreement, either Party may suspend this Agreement in whole or in part by written notification to the other Party through diplomatic channels. Such written notification shall not be made until after the Parties have engaged in a reasonable period of consultation without reaching a resolution and suspension shall take effect twenty days from the date of receipt of such notification. Such suspension may be lifted by the suspending Party upon written notification to the other Party. The suspension shall be lifted immediately upon receipt of such notification.

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

**Article 27: Territorial application**

1. This Agreement shall 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 applies 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 this 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 the month following receipt of the notification by the United States.

**Article 28: Duration of the Agreement**

This Agreement is concluded for an unlimited duration.

**Article 29: 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.

Done at _ this _ day of _ 201_, in two originals, in the English language. Pursuant to EU law, this Agreement shall also be drawn up by the EU in the Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Irish, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages. These additional language versions can be authenticated by an exchange of diplomatic notes between the United States and the European Union. In the case of divergence between authentic language versions, the English language shall prevail.