Council of the European Union

Brussels, 10 September 2026
(OR. en)

13003/26
ADD 1

Interinstitutional File:
2026/0280 (NLE)

IXIM 183
JAI 1122
VISA 103
DATAPROTECT 266
USA 30
JAIEX 59

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	10 September 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2026) 485 annex
Subject:	ANNEX to the Proposal for a Council decision on the conclusion of the Framework Agreement between the European Union and the United States of America on the reciprocal exchange of information for identity verification, and screening and vetting, relating to border procedures and applications for travel authorisations and visas

Delegations will find attached document COM(2026) 485 annex.

Encl.: COM(2026) 485 annex

EUROPEAN
COMMISSION

Brussels, 10.9.2026
COM(2026) 485 final

ANNEX

ANNEX

to the

Proposal for a Council decision

on the conclusion of the Framework Agreement between the European Union and the United States of America on the reciprocal exchange of information for identity verification, and screening and vetting, relating to border procedures and applications for travel authorisations and visas

Framework Agreement between the European Union and the United States of America on the reciprocal exchange of information for identity verification, and screening and vetting, relating to border procedures and applications for travel authorisations and visas

Table of Contents

Part 1 – Common Provisions
Article 1 – Objective of the Framework Agreement
Article 2 – Definitions
Article 3 – Scope of the Framework Agreement
Article 4 – Effect of the Framework Agreement

Part 2 – Principles and Conditions for the Information Exchange
Article 5 – Bilateral Agreements
Article 6 – Purpose of the Exchange of Information
Article 7 – Exchange of Information through an Automated Query
Article 8 – Confirmation of Risk
Article 9 – Procedure for Further Exchange of Additional Information
Article 10 – Single Points of Contact
Article 11 – Non-Derogation

Part 3 – Protection of Personal Information
Article 12 – Purpose and Use Limitation
Article 13 – Onward Sharing
Article 14 – Onward Transfers
Article 15 – Quality and Integrity of Information
Article 16 – Information Security
Article 17 – Notification of an Information Security Incident
Article 18 – Record Keeping
Article 19 – Retention Period
Article 20 – Special Categories of Personal Information
Article 21 – Automated Decisions
Article 22 – Access
Article 23 – Rectification
Article 24 – Administrative and Judicial Redress
Article 25 – Transparency
Article 26 – Effective Oversight

Part 4 – Institutional Framework
Article 27 – Joint Committee

Part 5 – Final Provisions
Article 28 – Consultations
Article 29 – Suspension
Article 30 – Territorial Application
Article 31 – Entry into Force, Duration, Amendment, and Termination
Article 32 – Provisional Application
Article 33 – Authentic Text

THE EUROPEAN UNION, hereinafter also referred to as the EU,

and

THE UNITED STATES OF AMERICA, hereinafter also referred to as the United States,

together hereinafter referred to as "the Parties",

SEEKING to encourage and enhance cooperation between the Parties in the spirit of transatlantic partnership;

INTENDING to establish a legal framework to facilitate the reciprocal exchange of information for the purposes of verification of identity, and screening and vetting, of individuals, with a view to preventing individuals who represent a serious and genuine risk to public security or public order, including on terrorism or criminal grounds, the ability to enter or stay in their territories;

HAVING REGARD for United Nations Security Council resolutions 1373 (2001), 1624 (2005), 2178 (2014), 2322 (2016), and, in particular, 2396 (2017) which requires Member States of the United Nations to develop and implement systems to collect biometric data in order to responsibly and properly identify terrorists, in compliance with domestic law and international human rights law, and which encourages Member States of the United Nations to share such information responsibly with each other, as appropriate;

MINDFUL that the United States and the European Union are committed to ensuring a high level of protection of personal information exchanged for the purposes of this Framework Agreement;

NOTING that the United States has in place Enhanced Border Security Partnerships with certain Member States of the EU, and UNDERSTANDING that the United States and those Member States intend to ensure compliance of those Partnerships with this Framework Agreement;

RESOLVED to strengthen, in the context of the bilateral Agreements on Enhancing Border Security through the Exchange of Information between the Member States of the EU and the United States, the exchange of identity information to prevent individuals seeking to cross their respective borders and stay in their territory from posing a risk to public security or public order;

MINDFUL that both Parties are committed to ensuring mutually beneficial exchanges of information needed to ensure the integrity and security of visa-free transatlantic travel through the Enhanced Border Security Partnership, but noting exchanges authorised in the bilateral Agreements on Enhancing Border Security through the Exchange of Information may be temporarily suspended in certain circumstances, including in the event of suspension of the visa-free travel;

RECOGNIZING that this Framework Agreement establishes common principles and safeguards for the reciprocal exchange of information under this Framework Agreement and does not preclude Member States of the EU and the United States from including additional types of information sharing cooperation in the bilateral Agreements on Enhancing Border Security through the Exchange of Information.

RECALLING the European Union's objective to explore ways to enhance information exchange for law enforcement and border management purposes with strategic partners and recognizing the Parties' shared objective for future expansion of cooperation in this area;

RECOGNIZING the principles of proportionality and necessity, and relevance and reasonableness, as implemented by the Parties in their respective legal frameworks, and CONSIDERING the level of information exchange between Member States of the EU;

EMPHASIZING that each Party should have in place a legal framework that provides individuals with effective judicial and non-judicial redress to identify and remedy instances where an individual's personal information has been processed and used in a manner inconsistent with Part 3 of this Framework Agreement, and ACKNOWLEDGING that it is for each Party to determine the type of remedies available, and that it is not required that each type of remedy be available in every instance;

REAFFIRMING the Parties' longstanding commitment to upholding the shared values and principles of democracy, the rule of law, and respect for human rights and fundamental freedoms, which underpin their domestic and international policies, and further reaffirming respect for the Universal Declaration of Human Rights and international human rights treaties to which the United States and Member States of the EU are parties, including the International Covenant on Civil and Political Rights, done at New York on December 16, 1966, and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, done at New York on December 10, 1984;

TAKING INTO ACCOUNT the Protocol on the Position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, and CONFIRMING that this Framework Agreement is not binding upon or applicable in relation to the Kingdom of Denmark;

TAKING INTO ACCOUNT the Protocol on the Schengen acquis integrated into the framework of the European Union, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, and CONFIRMING that the provisions of this Framework Agreement are not applicable in relation to Ireland;

HAVE AGREED AS FOLLOWS:

PART 1: COMMON PROVISIONS

Article 1
Objective of the Framework Agreement

1. The objective of this Framework Agreement is to enhance cooperation between the United States and the Member States of the EU in relation to the exchange of information on individuals crossing their respective external borders or applying for a travel authorisation or a visa to enter or stay in the territory of one of the Member States of the EU or of the United States, while ensuring a high level of protection of personal information.

2. In the pursuit of this objective, this Framework Agreement sets forth the framework for the exchange of information as well as the appropriate safeguards for the protection of personal information when transferred between the United States and the Member States of the EU.

3. This Framework Agreement in and of itself shall not be the legal basis for any transfers of personal information.

4. The exchange of information set out in this Framework Agreement shall be guided by the principle of reciprocity, which includes, in particular, similarity regarding maximum volume limits, type, and quality of information exchanged.

5. The exchange of information under Article 7 shall be based on a maximum volume of individuals to be screened, taking into account the capacity and technical limitations of the Competent Authorities, real volumes of travel, current risks, and reciprocity, to the extent determined in the bilateral Agreements on Enhancing Border Security through the Exchange of Information.

Article 2
Definitions

For the purposes of this Framework Agreement:

1. “Member State” means a Member State of the European Union;

2. “Union citizen” means any person holding the nationality of a Member State;

3. “U.S. national” or “national of the United States” means a citizen or national of the United States;

4. “Personal information” means information relating to an identified or identifiable natural person (an individual). 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;

5. “Processing of personal information” means any operation or set of operations involving collection, maintenance, use, alteration, organisation or structuring, disclosure or dissemination, or disposition;

6. “Special categories of personal information” means personal information revealing racial or ethnic origin, political opinions or religious or other beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and personal information concerning health or sexual life. An individual’s name, date of birth, place of birth, nationality/citizenship, or other basic biographic identity information shall not be deemed to constitute in themselves special categories of personal information;

7. “Competent Authority” means a public authority of the United States or of a Member State responsible for activities covered by this Framework Agreement, consistent with relevant designations in bilateral Agreements on Enhancing Border Security through the Exchange of Information between the Member States and the United States;
8. “Requesting Competent Authority” means the Competent Authority that initiates the query;

9. “Requested Competent Authority” means the Competent Authority that receives the query from the requesting competent authority;

10. “Travel authorisation” means an authorisation to travel and to seek admission to the territory of a Member State or of the United States for short or temporary stays for persons who are not subject to an obligation of being in possession of a visa, as defined in applicable law; and

11. “Visa” means an authorisation to travel or transit and to seek admission to the territory of a Member State or of the United States for short or temporary stays, as defined in applicable law.

Article 3
Scope of the Framework Agreement

1. This Framework Agreement shall apply to personal information of individuals transferred between the Competent Authorities of the United States and the Competent Authorities of the Member States for the purposes set forth in Article 6.

2. The Parties intend for the United States and the Member States to exchange information on U.S. nationals, Union citizens, and third country nationals. Should either the United States or a Member State be unable to categorically exchange information on its respective nationals or citizens, the other side is entitled to decide whether it will reciprocally refrain from exchanging information on all Union citizens or all U.S. nationals respectively.

3. For the purpose of paragraph 2, where a person is a Union citizen or is a U.S. national, or both, the transfer of personal information should be treated as a transfer of information on a citizen of a Member State or a national of the United States, regardless of whether that person holds one or more additional citizenships.

Article 4
Effect on the Framework Agreement

1. This Framework Agreement supplements, as appropriate, provisions regarding the protection of personal information in existing Enhanced Border Security Partnerships between the United States and Member States that address matters within the scope of this Framework Agreement. The United States shall undertake to adapt existing Enhanced Border Security Partnerships to ensure compliance with this Framework Agreement by working with the relevant Member States.

2. The Parties shall take all necessary measures to implement this Framework Agreement, including, in particular, their respective obligations under this Framework Agreement regarding access, rectification, and administrative and judicial redress for individuals provided herein. The protections and remedies set forth in this Framework Agreement shall benefit relevant individuals in the manner implemented in each Party's respective legal framework. 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 Competent Authorities, with respect to matters falling within the scope of this Framework Agreement, shall be deemed to comply with their respective data protection legislation restricting or conditioning international transfers of personal information, and no further authorisation under such legislation shall be required.

4. Except as provided in paragraph 1, nothing in this Framework Agreement shall be construed to limit or prejudice the provisions of any treaty, other agreement or arrangement, including mutual legal assistance agreements and agreements on enhancing cooperation in preventing and combatting serious crime, working law enforcement relationships, or domestic law allowing for information sharing between the United States and the Member States.

PART 2: PRINCIPLES AND CONDITIONS FOR THE INFORMATION EXCHANGE

Article 5
Bilateral Agreements

The exchange of information under this Framework Agreement may only take place to the extent authorised and further specified in bilateral Agreements on Enhancing Border Security through the Exchange of Information between the Member States and the United States (hereinafter "bilateral agreements") and only to the extent that those bilateral agreements:

a) include provisions necessary to comply with the conditions for the exchange of information set out in this Framework Agreement;

b) identify specific national information systems that are relevant for the objective described in Article 1 and the purposes described in Article 6, from which information is to be exchanged under this Framework Agreement and in accordance with applicable domestic laws (hereinafter "national information systems"); and

c) include provisions on suspension of the bilateral agreements, for reasons including suspension of visa-free travel.

Article 6
Purpose of the Exchange of Information

Personal information shall only be exchanged under this Framework Agreement for the purposes of verification of identity, and screening and vetting, of individuals needed to determine whether their entry or stay would pose a serious and genuine risk to public security or public order.

Article 7
Exchange of Information through an Automated Query (first step)

1. During the assessment of an application for a travel authorisation or visa or during border checks, the Requesting Competent Authority may submit an automated query in relation to an individual where, during the examination of the individual, there is reason to believe that the entry or stay could pose a serious and genuine risk to public security or public order. This may in particular be the case: where there are indications of identity fraud or misuse of identities; where there are doubts as to the authenticity and validity of the travel documents; where there are indications that an application for a visa contains fraudulent or false information; where there are risk assessments and scenarios identifying risk on the basis of trend analysis of suspicious activity, law enforcement cases, or criminal intelligence; or where information about the concerned individual exists in the national information systems of the Requesting Competent Authority.

2. While carrying out their activities referred to in paragraph 1, the Competent Authorities shall not arbitrarily and unjustifiably discriminate against individuals, in particular, on the grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.

3. Subject to the conditions set out in paragraph 1 and 2 above, the Requesting Competent Authority may submit an automated query in relation to an individual where there is a nexus between the individual and the State of the Requested Competent Authority, including where the individual is a citizen/national, is a current or former resident, or has previously stayed or applied to stay on the territory of the State of the Requested Competent Authority.

4. An automated query may only be initiated when the Requesting Competent Authority is also conducting searches against its own national information systems.

5. When submitting an automated query, the Requesting Competent Authority shall include a unique reference number that identifies the individual and/or the query and an indicator of the nature of the Requesting Competent Authority's encounter with the individual and may use the following personal information:

a) the identity information included in the application or in the travel document, such as the surname (family name), first name or names (given names), the date of birth, national ID number, and/or

b) the fingerprints of an individual.

6. Fingerprint data may only be used for the submission of the automated query if the relevant bilateral agreement requires the Requesting Competent Authority to ensure that the fingerprint data used in the query are of sufficient quality for automated comparison.

7. In case of a positive correspondence (match) with information held in its national information systems, the Requested Competent Authority shall transfer to the Requesting Competent Authority through the automated process:

a) the confirmation of such a match, and

b) alphanumeric data for the identification of an individual, such as first name, last name, and date of birth.

8. In case of a positive correspondence (match) with information held in its national information systems, the Requested Competent Authority may transfer to the Requesting Competent Authority through the automated process, where available and shareable under domestic law, photographs for the identification of an individual.

9. Under this Article, the Requested Competent Authority may only transfer personal information that is adequate, relevant, and limited to what is needed for the identification of the individual.

Article 8
Confirmation of Risk

1. Should the procedure described in Article 7 generate a positive correspondence (match), the Requested Competent Authority, to the extent authorised and further specified in the relevant bilateral agreement, shall assess without delay, based on all relevant factors, whether the positive correspondence is related to a risk set forth in Article 6. Such factors may include criminal convictions, terrorist threats or immigration violations, including their nature, seriousness and timing.

2. The Requested Competent Authority shall send without delay a confirmation whether there is information of potential interest related to a risk set forth in Article 6, which may be requested under the procedure of Article 9, and its nature, by indicating the relevant factor or factors referred to in paragraph 1.

3. The sharing of information pursuant to this Article may only take place to the extent that the relevant bilateral agreement establishes the procedures for sharing and the expected content of that communication, in accordance with applicable domestic law and consistent with the technical capabilities of the Requested Competent Authority.

Article 9
Procedure for Further Exchange of Additional Information (second step)

1. Should the procedure described in Article 7 show a positive correspondence (match) and after the procedures described in Article 8 have been completed, the Requesting Competent Authority may request additional information on the same individual for the purposes set forth in Article 6 to the extent authorised in the relevant bilateral agreement.

2. Subject to the safeguards for the protection of personal information set out in Part 3 of this Framework Agreement, the Requested Competent Authority may transfer the additional information requested by the Requesting Competent Authority.

3. The exchange of additional information may only take place to the extent that the relevant bilateral agreement specifies the national information systems from which information may be exchanged, the categories of information that the Requested Competent Authority may transfer, and the procedures for such transfer in accordance with applicable domestic law.

4. With the exception of biometric data for the purpose of uniquely identifying a natural person, special categories of personal information may only be transferred under this Article where particularly relevant to achieve the purposes set forth in Article 6.

5. The exchange of additional information may only take place to the extent that the relevant bilateral agreement establishes conditions for the exchange and only after a human assessment of compliance with those conditions by the Requested Competent Authority, and in accordance with applicable domestic law.

6. In the case of a positive correspondence (match) described in Article 7 and after the procedures described in Article 8 have been completed, the Requested Competent Authority may request available alphanumeric and contextual data on the same individual from the Requesting Competent Authority exclusively for ensuring accuracy and for auditing existing records on the individual concerned. The Requesting Competent Authority shall respond consistent with any relevant procedures provided in the bilateral agreements and in accordance with applicable domestic law.

Article 10
Single Points of Contact

The Competent Authorities shall designate single points of contact for the exchange of personal information under this Framework Agreement.

Article 11
Non-Derogation

The exchange of information under this Framework Agreement shall be without prejudice to the invocation by the Requested Competent Authority of grounds to refuse a request available

pursuant to a bilateral agreement or arrangement, such as where the response risks jeopardizing ongoing investigations or would prejudice the State of the Requested Competent Authority's sovereignty, security, public order, or if the response would conflict with applicable domestic law or international obligations.

PART 3: PROTECTION OF PERSONAL INFORMATION

Article 12
Purpose and Use Limitation

1. Personal information received under this Framework Agreement shall be processed for the purposes set forth in Article 6.

2. The further processing of personal information under this Framework Agreement shall not be incompatible with the purposes for which it was transferred.

3. Compatible processing includes further processing for purposes of preventing an immediate and serious threat to public security, further processing to report to public oversight authorities such as those listed in Article 26, and where further processing is directly related to the purposes for the exchange of information under this Framework Agreement. All such further processing shall respect the other provisions of this Framework Agreement, in particular its Articles 15 and 19. This paragraph is without prejudice to the application of treaties, agreements, or arrangements mentioned in Article 4, paragraph 4, such as mutual legal assistance agreements.

4. This Article shall not prejudice the ability of the Requested 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 such conditions, the Requesting Competent Authority shall comply with them. The Requested Competent Authority may also require the Requesting Competent Authority to give information on the use made of the transferred information.

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

Article 13
Onward Sharing

1. All processing of personal information exchanged under this Framework Agreement by other national law enforcement, regulatory, or administrative authorities shall respect the other provisions of Part 3 of this Framework Agreement.

2. The Parties shall have in place measures to promote accountability for processing personal information within the scope of the Framework Agreement by their Competent Authorities, and any 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 Framework Agreement, and of the conditions that may have been imposed by the Requested Competent Authority pursuant to Article 12, paragraph 4. Serious misconduct shall be addressed through appropriate and dissuasive criminal, civil, or administrative sanctions. Such measures shall include, as appropriate, discontinuation of transfer of personal information to authorities of constituent territorial entities of the Parties not covered by this Framework Agreement that have not effectively protected personal information, taking into account the purpose of this Framework Agreement, and in particular, the purpose and use limitations and onward transfer provisions of this Framework Agreement.

Article 14
Onward Transfers

1. Personal information received from the Requested Competent Authority pursuant to this Framework Agreement may be transferred to public authorities in third countries or to international organisations only where the prior consent of the Requested Competent Authority has been obtained.

2. When granting its consent to an onward transfer of personal information, the Requested Competent Authority shall take due account of all relevant factors, including the purpose for which the personal information was initially transferred and whether the third country or international organisation with which the information is to be shared ensures an appropriate level of protection of personal information.

Article 15
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 23;

b) where the Requested Competent Authority becomes aware of significant doubts as to the relevance, timeliness, completeness, or accuracy of such personal information it has transferred, it shall, where feasible, advise the Requesting Competent Authority thereof; and

c) where the Requesting Competent Authority becomes aware of significant doubts as to the relevance, timeliness, completeness, or accuracy of personal information received, it shall, where feasible, advise the Requested Competent Authority thereof.

Article 16
Information Security

1. The Competent Authorities shall ensure that they have in place appropriate technical, security and organisational arrangements for the protection of personal information against all of the following:

    a) accidental or unlawful destruction;

    b) accidental loss; and

    c) unauthorised disclosure, alteration, access, or other processing.

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

Article 17
Notification of an Information Security Incident

1. Upon discovery of an incident involving accidental loss or destruction, or unauthorised access, disclosure, alteration, or other processing of personal information, in which there is a significant risk of damage, the Requesting Competent Authority shall promptly assess the likelihood and scale of damage to individuals and promptly take appropriate action to mitigate any such damage.

2. Action to mitigate damage shall include a notification to the Requested Competent Authority. Such a notification may:

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

    b) be delayed or omitted when it may endanger national security;

    c) be delayed when it 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 offences;

    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 each other concerning the incident and the response thereto.

Article 18
Record Keeping

1. The Competent Authorities shall have in place effective methods of demonstrating the lawfulness of processing of personal information, which may include the use of logs containing a clear and specific purpose of each query and the logging of processing operations related to the exchange, as well as other forms of records.

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

Article 19
Retention Period

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 individuals, and other applicable legal considerations. The Parties shall provide procedures for at least an annual review of the retention period with a view to determining whether changed circumstances require further modification of the applicable period.

Article 20
Special Categories of Personal Information

1. Processing of special categories of personal information shall only take place under appropriate safeguards in accordance with law.

2. The appropriate safeguards referred to in paragraph 1 may include the following protective measures:

    a) restricting the purposes for which the information may be processed, such as allowing the processing only on a case-by-case basis;

    b) masking, deleting, or blocking the information after effecting the purpose for which it was processed;

    c) restricting personnel permitted to access the information;

    d) requiring specialised training for personnel who access the information;

    e) requiring supervisory approval to access the information.

3. These safeguards shall duly take into account the nature of the personal information, particular sensitivities of the information, and the purpose for which the information is processed.

Article 21
Automated Decisions

Decisions producing significant adverse actions concerning the relevant interests of individuals may not be based solely on the automated processing of personal information without human involvement, unless authorised under the Parties' respective legal frameworks, and with appropriate safeguards that include the possibility to obtain human intervention.

Article 22
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 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 offences or the execution of criminal penalties; or

    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 authorise, where permitted under 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 authorised representative as set forth in paragraph 4, the reasons for the denial or restriction of access.

Article 23
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 Requesting Competent Authority concludes following:

    a) a request under paragraph 1;

    b) notification by the Requested Competent Authority; or

    c) its own investigations or inquiries;

    that information it has received under this Framework 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 authorise, where permitted under 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 authorised representative as set forth in paragraph 3, a response setting forth the basis for the denial or restriction of correction or rectification.

Article 24
Administrative and Judicial Redress

The Parties shall have in place effective administrative and judicial remedies to provide redress for individuals whose personal information has been processed and used in a manner inconsistent with Part 3 of this Framework Agreement as set forth under each Party's respective legal framework and in accordance with Article 4, paragraph 2.

Article 25
Transparency

1. The Parties shall ensure that notice is provided 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 22, paragraph 2 (a) through (f).

Article 26
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 Part 3 of this Framework Agreement; and

    c) have the power to refer violations of law related to Part 3 of this Framework Agreement for prosecution or disciplinary action when appropriate.

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

3. The United States shall provide for oversight under this Article cumulatively through more than one authority, which may include 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.

PART 4: INSTITUTIONAL FRAMEWORK

Article 27
Joint Committee

1. A Joint Committee consisting of representatives of the Parties shall meet at least once a year to conduct consultations relating to this Framework Agreement and to review its implementation.

2. The Joint Committee shall be co-chaired by a representative of the European Union and a representative of the United States.

3. A Party may also request a meeting to seek to address questions related to the interpretation or application of this Framework Agreement.

4. The Joint Committee shall:

    a) Monitor the effective implementation of this Framework Agreement, including by carrying out periodic joint reviews of the implementation of this Framework Agreement no later than three years from the date of the entry into force of this Framework Agreement, and thereafter on a regular basis, to assess the effectiveness, and proportionality or reasonableness, of the volume and reciprocity of the exchange of information in relation to the purposes of the

implementation of this Framework Agreement. To this end, the Parties shall ensure that the Joint Committee receives statistics collected by the Member States and the United States including the number and nature of queries, the number and percentage of matches, and the timeliness of responses processed under this Framework Agreement;

b) Hold consultations consistent with Article 28; and

c) Provide guidance regarding how the Framework Agreement should be interpreted and implemented, where appropriate, and facilitate specific aspects of cooperation based on this Framework Agreement.

5. The Joint Committee's working methods shall be by consensus.

PART 5: FINAL PROVISIONS

Article 28
Consultations

Any dispute regarding the interpretation and implementation of this Framework Agreement shall be resolved by consultations between the Parties, which may include consultations in the Joint Committee, and shall not be referred to any national or international tribunal or third party for settlement.

Article 29
Suspension

1. In the event of a material breach of this Framework Agreement, either Party may suspend this Framework 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 Framework Agreement, personal information falling within the scope of this Framework Agreement and transferred prior to its suspension shall continue to be protected in accordance with the safeguards of this Framework Agreement.

3. In the event of suspension of this Framework Agreement, cooperation between the United States and Member States under the bilateral agreements that is dependent on this Framework Agreement is expected to be suspended, consistent with those bilateral agreements. The bilateral agreements are expected to include a suspension provision specifying that elements of the bilateral agreements that fall under this Framework Agreement will be suspended should this Framework Agreement be suspended.

Article 30
Territorial Application

1. Subject to paragraph 2, this Framework Agreement shall apply, of the one part, to the territory in which the Treaty on European Union and the Treaty on the Functioning of the European Union apply and under the conditions laid down in those Treaties, and, of the other part, to the territory of United States.

2. This Framework Agreement shall apply to the territory of Ireland only pursuant to a notification by the European Union to United States to that effect. This Agreement shall not apply to the territory of the Kingdom of Denmark.

Article 31
Entry into Force, Duration, Amendment, and Termination

1. This Framework Agreement shall enter into force on the first day of the month following the date on which the Parties have notified each other in writing of the completion of their respective internal legal procedures for the entry into force of this Framework Agreement.

2. This Framework Agreement shall be in force for an indefinite period.

3. The Parties may agree, in writing, to amend this Framework Agreement.

4. Either Party may terminate this Framework Agreement by written notification to the other Party through diplomatic channels. Such termination shall take effect on the first day of the sixth month following the date of such notification.

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

6. In the event of termination of this Framework Agreement, cooperation between the United States and Member States under the bilateral agreements that is dependent on this Framework Agreement is expected to cease, consistent with those bilateral agreements. The bilateral agreements are expected to include a termination provision specifying that elements of the bilateral agreements that fall under this Framework Agreement will be terminated should this Framework Agreement be terminated.

Article 32
Provisional Application

The European Union and the United States may apply this Framework Agreement provisionally, as of the date of signature.

Article 33
Authentic Text

The signed English text of this Framework Agreement shall be the authentic text. This Framework Agreement is drawn up by the European Union also 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.

FOR THE EUROPEAN UNION:	**FOR THE UNITED STATES OF AMERICA:**
……	……
Place: …….	Place: …….
Date: ……..	Date: ……..