

AGREEMENT**between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program**

THE EUROPEAN UNION,

of the one part, and

THE UNITED STATES OF AMERICA,

of the other part,

Together hereinafter referred to as 'the Parties',

DESIRING to prevent and combat terrorism and its financing, in particular by mutual sharing of information, as a means of protecting their respective democratic societies and common values, rights, and freedoms;

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

RECALLING the United Nations conventions for combating terrorism and its financing, and relevant resolutions of the United Nations Security Council in the field of fighting terrorism, in particular United Nations Security Council Resolution 1373 (2001);

RECOGNISING that the United States Department of the Treasury's (U.S. Treasury Department) Terrorist Finance Tracking Program (TFTP) has been instrumental in identifying and capturing terrorists and their financiers and has generated many leads that have been disseminated for counter terrorism purposes to competent authorities around the world, with particular value for European Union Member States (Member States);

NOTING the importance of the TFTP in preventing and combating terrorism and its financing in the European Union and elsewhere, and the important role of the European Union in ensuring that designated providers of international financial payment messaging services make available financial payment messaging data stored in the territory of the European Union which are necessary for preventing and combating terrorism and its financing, subject to strict compliance with safeguards on privacy and the protection of personal data;

MINDFUL of Article 6(2) of the Treaty on European Union on respect for fundamental rights, the principles of proportionality and necessity concerning the right to respect for privacy and the protection of personal data under Article 8(2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms, the Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union;

STRESSING the common values governing privacy and the protection of personal data in the European Union and the United States of America (United States), including the importance which both Parties assign to due process and the right to seek effective remedies for improper government action;

NOTING the rigorous controls and safeguards utilised by the U.S. Treasury Department for the handling, use, and dissemination of financial payment messaging data pursuant to the TFTP, as described in the representations of the U.S. Treasury Department published in the *Official Journal of the European Union* on 20 July 2007 and the *Federal Register* of the United States on 23 October 2007, which reflect the ongoing cooperation between the United States and the European Union in the fight against global terrorism;

RECALLING that, to guarantee effective exercise of their rights, any person irrespective of nationality is able to lodge a complaint before an independent data protection authority, other similar authority, independent and impartial court or tribunal, to seek effective remedies;

MINDFUL that appropriate administrative or judicial redress is available under U.S. law for mishandling of personal data, including under the Administrative Procedure Act of 1946 (5 U.S.C. 701 et seq.), the Inspector General Act of 1978 (5 U.S.C. App.), the Implementing Recommendations of the 9/11 Commission Act of 2007 (42 U.S.C. 2000ee et seq.), the Computer Fraud and Abuse Act (18 U.S.C. 1030), and the Freedom of Information Act (5 U.S.C. 552), as amended, among others;

RECALLING that by law within the European Union customers of financial institutions and of providers of financial payment messaging services are informed that personal data contained in financial transaction records may be transferred to Member States' or third countries' public authorities for law enforcement purposes;

AFFIRMING that this Agreement does not constitute a precedent for any future arrangements between the United States and the European Union, or between either of the Parties and any State, regarding the processing and transfer of financial payment messaging data or any other form of data, or regarding data protection;

RECOGNISING that this Agreement does not derogate from the existing powers of data protection authorities in Member States to protect individuals with regard to the processing of their personal data; and

FURTHER AFFIRMING that this Agreement is without prejudice to other law enforcement or information sharing agreements or arrangements between the Parties or between the United States and Member States,

HAVE AGREED AS FOLLOWS:

Article 1

Purpose of Agreement

1. The purpose of this Agreement is to ensure, with full respect for the privacy, protection of personal data, and other conditions set out in this Agreement, that:

- (a) financial payment messaging and related data stored in the territory of the European Union by providers of international financial payment messaging services, that are jointly designated pursuant to this Agreement, are made available upon request by the U.S. Treasury Department for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; and
- (b) relevant information obtained through the TFTP is made available to law enforcement, public security, or counter terrorism authorities of Member States, or Europol or Eurojust, for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing.

2. The United States, the European Union, and its Member States shall take all necessary and appropriate measures within their authority to carry out the provisions and achieve the purpose of this Agreement.

Article 2

Scope of Application

Conduct Pertaining to Terrorism or Terrorist Financing

This Agreement applies to the obtaining and use of financial payment messaging and related data with a view to the prevention, investigation, detection, or prosecution of:

- (a) Acts of a person or entity that involve violence, or are otherwise dangerous to human life or create a risk of

damage to property or infrastructure, and which, given their nature and context, are reasonably believed to be committed with the aim of:

- (i) intimidating or coercing a population;
 - (ii) intimidating, compelling, or coercing a government or international organisation to act or abstain from acting; or
 - (iii) seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation;
- (b) A person or entity assisting, sponsoring, or providing financial, material, or technological support for, or financial or other services to or in support of, acts described in subparagraph (a); or
- (c) A person or entity aiding, abetting, or attempting acts described in subparagraphs (a) or (b).

Article 3

Ensuring Provision of Data by Designated Providers

The European Union shall ensure, in accordance with this Agreement, that entities jointly designated by the Parties under this Agreement as providers of international financial payment messaging services (Designated Providers) make available to the U.S. Treasury Department requested financial payment messaging and related data for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing (Provided Data).

*Article 4***U.S. Requests to Obtain Data from Designated Providers**

1. Pursuant to Article 8 of the Agreement on Mutual Legal Assistance between the European Union and the United States of America, signed at Washington on 25 June 2003, and the related bilateral mutual legal assistance instrument between the United States and the Member State in which the Designated Provider is either based or where it stores the requested data, the U.S. Treasury Department shall issue a request based on an ongoing investigation concerning a specific conduct referred to in Article 2 that has been committed or where there is, based on pre-existing information or evidence, a reason to believe that it could be committed. For this purpose, the U.S. Treasury Department shall be deemed to be an administrative authority to which assistance is available.

2. The request shall identify as clearly as possible data stored by a Designated Provider in the territory of the European Union that are necessary to this end. Data may include identifying information about the originator and/or recipient of the transaction, including name, account number, address, national identification number, and other personal data related to financial messages.

The request shall substantiate the necessity for the data and shall be tailored as narrowly as possible in order to minimise the amount of data requested, taking due account of geographic, threat and vulnerability analyses.

3. The request shall be transmitted by the U.S. Department of Justice to the central authority of the Member State either in which the Designated Provider is based or where it stores the requested data.

4. The United States shall simultaneously transmit a copy of the request to the central authority of the other Member State. The United States shall also simultaneously transmit a copy of the request to the national members of Eurojust of those Member States.

5. On receipt of the substantiated request in accordance with paragraph 2, the central authority of the requested Member State shall verify that the request accords with this Agreement and the applicable requirements of the bilateral mutual legal assistance agreement. Where the central authority has so verified, the request shall be transmitted to the competent authority for its execution under the law of the requested Member State.

If the request has been transmitted to the central authority of the Member State in which the Designated Provider is based, the

Member State where the data are stored shall give assistance to the execution of the request.

The requested measure shall be executed as a matter of urgency.

6. If the Designated Provider is not able to identify and produce the specific data that would respond to the request because of technical reasons, all potentially relevant data shall be transmitted in bulk, subject to Article 5(2), to the competent authority of the requested Member State.

7. The data shall be transferred between the designated authorities of the requested Member State and of the United States.

8. The European Union shall ensure that Designated Providers keep a detailed log of all data transmitted to the competent authority of the requested Member State for the purpose of this Agreement.

9. The data that have been transmitted lawfully on the basis of this provision may be searched for the purpose of other investigations concerning the types of conduct referred to in Article 2, with full respect for Article 5 of this Agreement.

*Article 5***Safeguards Applicable to the Processing of Provided Data**

1. The U.S. Treasury Department shall ensure that Provided Data are processed in accordance with the provisions of this Agreement.

2. The TFTP does not and shall not involve data mining or any other type of algorithmic or automated profiling or computer filtering. The U.S. Treasury Department shall ensure the protection of personal data by means of the following safeguards, which shall be applied without discrimination, in particular on the basis of nationality or country of residence:

(a) Provided Data shall be processed exclusively for the prevention, investigation, detection, or prosecution of terrorism or its financing;

(b) All searches of Provided Data shall be based upon pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing;

- (c) Each individual TFTP search of Provided Data shall be narrowly tailored, shall demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing, and shall be logged, including such nexus to terrorism or its financing required to initiate the search;
- (d) Provided Data shall be maintained in a secure physical environment, stored separately from any other data, with high-level systems and physical intrusion controls to prevent unauthorised access to the data;
- (e) Access to Provided Data shall be limited to analysts investigating terrorism or its financing and to persons involved in the technical support, management, and oversight of the TFTP;
- (f) No copies of Provided Data shall be made, other than for disaster recovery back-up purposes;
- (g) Provided Data shall not be subject to any manipulation, alteration, or addition and shall not be interconnected with any other database;
- (h) Only terrorist leads obtained through the TFTP under this Agreement shall be shared with law enforcement, public security, or counter terrorism authorities in the United States, European Union, or third States to be used for the purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing;
- (i) During the term of this Agreement, the U.S. Treasury Department shall undertake a review to identify all non-extracted data that are no longer necessary to combat terrorism or its financing. Where such data are identified, procedures to delete those data shall commence within two (2) months of the date that they are so identified and shall be completed as soon as possible thereafter but in any event not later than eight (8) months after identification, absent extraordinary technological circumstances;
- (j) If it transpires that financial payment messaging data were transmitted which were not requested, the U.S. Treasury Department shall promptly and permanently delete such data and shall inform the relevant Designated Provider and central authority of the requested Member State;
- (k) Subject to subparagraph (i), all non-extracted data received prior to 20 July 2007 shall be deleted not later than five (5) years after that date;
- (l) Subject to subparagraph (i), all non-extracted data received on or after 20 July 2007 shall be deleted not later than five (5) years from receipt; and
- (m) Information extracted from Provided Data, including information shared under subparagraph (h), shall be subject to the retention period applicable to the particular government authority according to its particular regulations and record retention schedules.

Article 6

Adequacy

Subject to ongoing compliance with the commitments on privacy and protection of personal data set out in this Agreement, the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the European Union to the United States for purposes of this Agreement.

Article 7

Spontaneous Provision of Information

1. The U.S. Treasury Department shall ensure the availability, as soon as practicable, to law enforcement, public security, or counter terrorism authorities of concerned Member States, and, as appropriate, to Europol within the remit of its mandate, of information obtained through the TFTP that may contribute to the investigation, prevention, detection, or prosecution in the European Union of terrorism or its financing. Any follow-on information that may contribute to the investigation, prevention, detection, or prosecution in the United States of terrorism or its financing shall be conveyed back to the United States on a reciprocal basis.

2. In order to facilitate the efficient exchange of information, Europol may designate a liaison officer to the U.S. Treasury Department. The modalities of the liaison officer's status and tasks shall be decided jointly by the Parties.

Article 8

EU Requests for TFTP Searches

Where a law enforcement, public security, or counter terrorism authority of a Member State, or Europol or Eurojust, determines that there is reason to believe that a person or entity has a nexus to terrorism as defined in Articles 1 to 4 of Council Framework Decision 2002/475/JHA as amended by Council Framework Decision 2008/919/JHA, such authority may request a search for relevant information obtained through the TFTP. The U.S. Treasury Department shall promptly conduct a search in accordance with Article 5 and provide relevant information in response to such requests.

*Article 9***Cooperation with Future Equivalent EU System**

In the event that an EU system equivalent to the U.S. TFTP is implemented in the European Union or in one or more of its Member States that requires financial payment messaging data stored in the United States to be made available in the European Union, the U.S. Treasury Department shall actively pursue, on the basis of reciprocity and appropriate safeguards, the cooperation of any relevant international financial payment messaging service providers which are based in the territory of the United States.

*Article 10***Joint Review**

1. The Parties shall jointly review, at the request of one of the Parties and at any event after a period of six (6) months, the implementation of this Agreement with particular regard to verifying the privacy, protection of personal data, and reciprocity provisions set out in this Agreement. The review shall include a proportionality assessment of the Provided Data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing.

2. In the review, the European Union shall be represented by the Presidency of the Council of the European Union, the European Commission, and two representatives of data protection authorities from Member States, at least one of which shall be from a Member State where a Designated Provider is based. The United States shall be represented by the U.S. Treasury Department.

3. For purposes of the review, the U.S. Treasury Department shall ensure access to relevant documentation, systems, and personnel, as well as precise data relating to the number of financial payment messages accessed and the number of occasions on which leads have been shared. The Parties shall jointly determine the modalities of the review.

*Article 11***Redress**

1. Any person has the right to obtain, following requests made at reasonable intervals, without constraint and without excessive delay or expense, confirmation from his or her data protection authority whether all necessary verifications have taken place within the European Union to ensure that his or her data protection rights have been respected in compliance with this Agreement, and, in particular, whether any processing of his or her personal data has taken place in breach of this Agreement. Such right may be subject to necessary and proportionate measures applicable under national law, including for the protection of public security or national security or to avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences, with due regard for the legitimate interest of the person concerned.

2. The Parties shall take all reasonable steps to ensure that the U.S. Treasury Department and any relevant Member State promptly inform one another, and consult with one another and the Parties, if necessary, where they consider that personal data have been processed in breach of this Agreement.

3. Any person who considers his or her personal data to have been processed in breach of this Agreement is entitled to seek effective administrative and judicial redress in accordance with the laws of the European Union, its Member States, and the United States, respectively.

*Article 12***Consultation**

1. The Parties shall, as appropriate, consult to enable the most effective use to be made of this Agreement, including to facilitate the resolution of any dispute regarding the interpretation or application of this Agreement.

2. The Parties shall take measures to avoid the imposition of extraordinary burdens on one another through application of this Agreement. Where extraordinary burdens nonetheless result, the Parties shall immediately consult with a view to facilitating the application of this Agreement, including the taking of such measures as may be required to reduce pending and future burdens.

3. The Parties shall immediately consult in the event that any third party, including an authority of another country, challenges or asserts a legal claim with respect to any aspect of the effect or implementation of this Agreement.

*Article 13***Non-derogation**

This Agreement is not intended to derogate from or amend the laws of the United States or the European Union or its Member States. This Agreement does not create or confer any right or benefit on any other person or entity, private or public.

*Article 14***Termination**

1. Either party may suspend or terminate this Agreement at any time by notification through diplomatic channels. Suspension shall take effect 10 days from the date of receipt of such notification. Termination shall take effect 30 days from the date of receipt of such notification.

2. Notwithstanding the suspension or termination of this Agreement, all data held by the U.S. Treasury Department pursuant to this Agreement shall continue to be processed in accordance with this Agreement.

*Article 15***Final Provisions**

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

2. This Agreement shall apply provisionally from 1 February 2010, until its entry into force, subject to paragraph 3.

3. Unless previously terminated in accordance with Article 14 or by agreement of the Parties, this Agreement shall expire and cease to have effect on 31 October 2010.

4. As soon as the Treaty of Lisbon enters into force, the Parties shall endeavour to conclude a long-term agreement to succeed this Agreement.

5. Done at Brussels this day 30 of November 2009, in two originals, in the English language. This Agreement shall also be drawn up in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, and Swedish languages. Upon approval by both Parties, these language versions shall be considered equally authentic.
