

EU/USA Agreement: processing and transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Program

2010/0178(NLE) - 24/06/2010 - Legislative proposal

PURPOSE: to conclude a new 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.

PROPOSED ACT: Council Decision.

IMPACT ANALYSIS: no impact analysis was carried out.

LEGAL BASIS: Articles 87(2)(a) and 88 (2), in conjunction with Article 218 (6)(a) of the Treaty on the Functioning of the European Union (TFEU).

CONTENT: this proposal sets out the text of the new Agreement between the EU 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 main elements of the this Agreement can be summarised as follows:

Purpose of the Agreement: like the previous version, 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:

- financial payment messages referring to financial transfers 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 provided to the U.S. Treasury Department for the exclusive purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing;
- relevant information obtained through the TFTP is provided 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.

Data concerned: the 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 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:

- intimidating or coercing a population;
- intimidating, compelling, or coercing a government or international organisation to act or abstain from acting;
- seriously destabilizing or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation.

It may also concern data from a person or entity assisting, sponsoring, or providing financial, material, or technological support for, or financial or other services to or in support of, abovementioned acts.

Since the new systems architecture of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (hereinafter referred to as the "designated provider") became operational on 1 January 2010, a significant volume of the data which were previously received by the U.S. Treasury Department under the TFTP, have not been available, undermining the benefits of the TFTP not least for the European Union.

Ensuring Provision of Data by Designated Providers: the Agreement stipulates that the Parties, jointly and individually, shall ensure that entities jointly designated by the Parties under this Agreement as providers of international financial payment messaging services ("Designated Providers", i.a. Society for Worldwide Interbank Financial Telecommunication - SWIFT-) provide to the U.S. Treasury Department requested financial payment messaging and related data which are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing ("Provided Data").

U.S. Requests to Obtain Data from Designated Providers: for the purposes of this Agreement, the U.S. Treasury Department shall serve production orders (Requests), under authority of U.S. law, upon a Designated Provider present in the territory of the United States in order to obtain data necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing that are stored in the territory of the European Union.

The Request (together with any supplemental documents) shall:

- identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing;
- clearly substantiate the necessity of the data;
- be tailored as narrowly as possible in order to minimize the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat, and vulnerability analyses;
- not seek any data relating to the Single Euro Payments Area.

A copy of the Request shall be sent to Europol. Once Europol has confirmed that the Request complies with the requirements of the Agreement, the Request shall have binding legal effect as provided under U.S. law, within the European Union as well as the United States. The Designated Provider is thereby authorised and required to provide the data to the U.S. Treasury Department.

Safeguards Applicable to the Processing of Provided Data: the U.S. Treasury Department shall ensure that Provided Data are processed in

accordance with the provisions of this Agreement The TFTP shall avoid data mining or any other type of algorithmic or automated profiling or computer filtering. The U.S. Treasury Department shall ensure that Provided Data are processed in accordance with the provisions of this Agreement. The U.S. Treasury Department shall ensure the protection of personal data by means of a series of safeguards set out in the Agreement.

Provisions on data security and integrity are also laid down in the Agreement.

Necessary and Proportionate Processing of Data: 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. Provided Data may include identifying information about the originator and/or recipient of a transaction, including name, account number, address, and national identification number. The Parties recognize the special sensitivity of personal data revealing racial or ethnic origin, political opinions, or religious or other beliefs, trade union membership, or health and sexual life (?sensitive data?). In the exceptional circumstance that extracted data were to include sensitive data, the U.S. Treasury Department shall protect such data in accordance with the safeguards and security measures set forth in this Agreement and with full respect and taking due account of their special sensitivity.

Retention and Deletion of Data: during the term of this Agreement, the U.S. Treasury Department shall undertake an ongoing and at least annual evaluation to assess the data retention periods to ensure that they continue to be no longer than necessary to combat terrorism or its financing. Where such data are identified, the U.S. Treasury Department shall permanently delete them as soon as technologically feasible. 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. All non-extracted data received prior to 20 July 2007 shall be deleted not later than 20 July 2012. All non-extracted data received on or after 20 July 2007 shall be deleted not later than five years from receipt. Not later than three years from the date of entry into force of this Agreement, the European Commission and the U.S. Treasury Department shall prepare a joint report regarding the value of TFTP Provided Data, with particular emphasis on the value of data retained for multiple years and relevant information obtained from the joint review conducted pursuant to the Agreement.

Onward Transfer: provisions are laid down as regards the onward transfer of information extracted from the Provided Data. Such information shall be shared for lead purposes only and for the exclusive purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing. Where the U.S. Treasury Department is aware that such information involves a citizen or resident of a Member State, any sharing of the information with the authorities of a third country shall be subject to the prior consent of competent authorities of the concerned Member State or pursuant to existing protocols on such information sharing between the U.S. Treasury Department and that Member State, except where the sharing of the data is essential for the prevention of an immediate and serious threat to public security of a Party to this Agreement, a Member State, or a third country.

Spontaneous Provision of Information: the U.S. Treasury Department shall ensure the availability, as soon as practicable and in the most expedient manner, to law enforcement, public security, or counter terrorism authorities of concerned Member States, and, as appropriate, to Europol and Eurojust, within the remit of their respective mandates, of information obtained through the TFTP that may contribute to the investigation, prevention, detection, or prosecution by the European Union of terrorism or its financing. Any follow-on information that may contribute to the investigation, prevention, detection, or prosecution by the United States of terrorism or its financing shall be conveyed back to the United States on a reciprocal basis and in a reciprocal manner.

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 or its financing, such authority may request a search for relevant information obtained through the TFTP. The U.S. Treasury Department shall promptly conduct a search and provide relevant information in response to such requests.

Cooperation with Future Equivalent EU System: during the course of this Agreement, the European Commission will carry out a study into the possible introduction of an equivalent EU system allowing for a more targeted transfer of data. If, following this study, the European Union decides to establish an EU system, the United States shall cooperate and provide assistance and advice to contribute to the effective establishment of such a system.

Monitoring of Safeguards and Controls: compliance with the strict counter terrorism purpose limitation and the other safeguards set out in the Agreement shall be subject to independent monitoring and oversight. The oversight shall be subject to ongoing monitoring, including of the independence of the oversight, by an independent person appointed by the European Commission in agreement with the United States. Such oversight, subject to appropriate security clearances, shall include the authority to review in real time and retrospectively all searches made of the Provided Data, the authority to query such searches and, as appropriate, to request additional justification of the terrorism nexus. In particular, independent overseers shall have the authority to block any or all searches if it appears that one or more searches have been made in breach of the Agreement.

Joint Review: at the request of one of the Parties and at any event after a period of six months from the entry into force of this Agreement, the Parties shall jointly review the safeguards, controls and reciprocity provisions set out in this Agreement. Following the review, the European Commission will present a report to the European Parliament and the Council on the functioning of the Agreement.

Transparency: the U.S. Treasury Department shall post on its public website detailed information concerning the TFTP and its purposes, including contact information for persons with questions. In addition it shall post information about the procedures available for the exercise of the rights, including the availability of administrative and judicial redress as appropriate in the United States regarding the processing of personal data received.

Right of Access: measures are laid stipulating that any person has the right to obtain, following requests made at reasonable intervals, without constraint and without excessive delay, at least a confirmation transmitted through his or her data protection authority in the European Union as to whether that person's data protection rights have been respected. Disclosure to a person of his or her personal data processed under this Agreement may be subject to reasonable legal limitations applicable under national law to safeguard the prevention, detection, investigation, or prosecution of criminal offences, and to protect public or national security, with due regard for the legitimate interest of the person concerned. In the case that access to personal data is refused or restricted, such refusal or restriction shall be explained in writing and provide information on the means available for seeking administrative and judicial redress in the United States.

Right to Rectification, Erasure, or Blocking: any person has the right to seek the rectification, erasure, or blocking of his or her personal data processed by the U.S. Treasury Department pursuant to this Agreement where the data are inaccurate or the processing contravenes this Agreement. Other provisions are laid down to ensure that data received have been rectified, erased, or blocked, and whether the data subject's rights have been duly respected.

Redress: specific provisions are laid down as regards redress. 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. For this purpose and as regards data transferred to the United States pursuant to this Agreement, the U.S. Treasury Department shall treat all persons equally in the application of its administrative process, regardless of nationality or country of residence.

Consultation: it is provided that the Parties shall, as appropriate, consult each other 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. 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.

Suspension or Termination: the Agreement stipulates that either Party may suspend the application of this Agreement with immediate effect, in the event of breach of the other Party's obligations under this Agreement, by notification through diplomatic channels. Either Party may terminate this Agreement at any time by notification through diplomatic channels. Termination shall take effect six months from the date of receipt of such notification. The Parties shall consult prior to any possible suspension or termination in a manner which allows a sufficient time for reaching a mutually agreeable resolution.

Territorial application: the Agreement will only apply to Denmark, the United Kingdom, or Ireland if the European Commission notifies the United States in writing that Denmark, the United Kingdom, or Ireland has chosen to be bound by the Agreement.