Brussels, 24.3.2010
SEC(2010)315 final

RESTREINT
UE RECOMMENDATION FROM THE COMMISSION TO THE COUNCIL to authorize the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing.

After the 11 September 2001 terrorist attacks, the United States Department of the Treasury developed the "Terrorist Finance Tracking Program" ("TFTP"), at the time a secret program under which the Treasury Department required, by means of administrative subpoenas, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in the United States to transfer to the Treasury Department limited sets of financial messaging data which transit over SWIFT's financial messaging network. The majority of these data originated in EU Member States and referred to intra EU transactions or international financial transactions not concerning the US. In mid 2006 U.S. media disclosed the existence of the TFTP, which attracted considerable criticism of the Treasury Department's program notably from the European Parliament and Member State Data Protection Authorities.

In early 2007, the Presidency of the Council of the European Union and the European Commission engaged in discussions with the U.S. Treasury-Department concerning the latter's processing of EU-originating personal data accessed under the TFTP. As a direct consequence of these discussions, the Treasury Department made a series of unilateral commitments to the European Union in June 2007 ("the TFTP Representations")[1]. The TFTP Representations expressly limit the Treasury's processing of EU-originating personal data accessed pursuant to the TFTP. Limitations include, for example, that data will be processed exclusively for counterterrorism purposes, that data can only be accessed if there is a pre-existing terrorism nexus (i.e. no data mining) and an obligation to delete data after a certain period. In addition, the TFTP Representations state that the Commission may appoint an "eminent European person" who will verify and report to the Commission on U.S. Treasury compliance with its commitments.

In March 2008 the Commission announced that it had designated Judge Jean-Louis Bruguière as the SWIFT eminent European person. Judge Bruguière completed his first report in December 2008. The Report which was presented to the Justice and Home Affairs Council in February 2009 and to the European Parliament's Civil Liberties Committee in February and September 2009, finds that the U.S. Treasury Department complies with the commitments set out in 'the

[1] The TFTP Representations were acknowledged by the European Union by letter of 29 June 2007. The TFTP Representations and EU letter of acknowledgment were published in OJ C 166, 20.7.2007, p.18 and OJ C 166, 20.7.2007, P.26.

TFTP Representations. The Report further concludes that the TFTP has generated considerable value for Member State authorities' investigation of terrorism who have been the main beneficiaries of TFTP-derived Information.

On 1 February 2010 a second report of Judge Bruguière, which confirmed the value of the TFTP as much as the U.S. Treasury Department's compliance with the safeguards set out in the TFTP Representations, was made available to the European Parliament and the Council.

SWIFT is currently the market leader in the provision of international financial payment messaging services, Until the end of 2009, SWIFT stored all FIN [2]messages on two identical ("minor") servers, located in Europe and the United States, On I January- 2010 SWIFT implemented its new messaging architecture consisting of two processing zones, namely a European and a transatlantic zone.

Under SWIFT's new architecture, the European zone consists of the current European operating centre accompanied by a new operating centre based in Switzerland. A key element of this new architecture is that ultra-European zone messages will only be processed and stored within their zone of origin. Accordingly, financial transaction messages carried over the SWIFT network and which are internal to the EEA and Switzerland will remain within the European zone. Inter-zone traffic will be stored at both, the sending and receiving zones. Countries other than EEA, Switzerland and the U.S. may opt to have their traffic stored within one or the other zone. A number of non-European countries have requested to have their data processed and stored within the European zone.

As far as the TFTP is concerned, the net effect of SWIFTs new architecture is that more than 50% of the data which formed the basis of TFTP subpoenas are no longer stored in the United States as from end 2009.
For this reason and to ensure the continuity of the TFTP, the JHA Council of 30 November 2009 had authorized the Presidency of the Council of the European Union to sign an interim agreement between the EU and the United States on the processing and transfer of Financial Messaging Data from the EU to the U.S. for purposes of the TFTP. The interim agreement, also signed on 30 November 2009, had a maximum duration of 9 months.

On 11 February 2010 the European Parliament withheld its consent to the agreement, which had become a prerequisite pursuant to Article 218(6}(a) TFEU after the entry into force of the Lisbon Treaty on 1 December 2009. Consequently the interim agreement was not concluded.

The removal of banking secrecy provisions, in appropriate circumstances, is vital in order to combat the financing of terrorism. As confirmed by the European Council already in October 2000, fiscal and banking secrecy should not provide barriers to investigations on money-laundering and international cooperation. A

[2] " FIN" messages are *one* of a range of financial messaging services offered by SWIFT. It is FIN messages which are the subject of TFTP subpoenas.

Protocol to the EU Mutual Legal Assistance Convention now ensures that banking secrecy provisions are not invoked as a reason to refuse a request for assistance from another Member State.

The long-term agreement shall address the concerns set out in the European Parliament's Resolution of 17 September 2009, particularly with regard to the protection of personal data.

In case the EU decides to establish a TFTP, the agreement shall provide for cooperation and assistance between the parties.

The Terrorist Finance Tracking Programme has generated a significant number of intelligence leads which have benefitted Member State services in the fight against terrorism in the European Union[3]. There is currently no equivalent of the TFTP in the European Union.

The European Union and the United States Government work together to prevent and combat terrorism while respecting fundamental rights, notably the protection of personal data as well as the protection of business secrets; it should also ensure legal certainty for the transfer of relevant financial-messaging data to the U.S. Treasury Department while ensuring protection of personal data for the exclusive purpose of the US Treasury Department's TFTP and preventing any kind of industrial espionage.

Therefore this solution should be applied homogeneously throughout the European Union.

Appropriate safeguards are necessary to ensure the respect of the fundamental right to the protection of personal data as a precondition for making available relevant data in the knowledge that they may be exclusively processed for counter-terrorism purposes and to ensure legal certainty for concerned financial messaging operators. Such safeguards must ensure full respect for fundamental rights enshrined in Article 6 of the Treaty on European Union, the right of the protection of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union and for the principles of necessity and proportionality regarding the fundamental rights to the protection of personal data and the respect for private and family life respectively set out in Article 8 of the European Convention on Human Rights and Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union. The envisaged agreement will ensure respect for these rights and safeguards. Moreover, no extracted

---

[3] The "eminent European person" Report of December 2008 contains various examples of where TFTP-derived Intelligence has been shared with EU Member State services in connection with the investigation, prevention and prosecution of terrorism in the European Union. The Report further states that United States authorities have shared approximately 1400 TFTP derived leads with Member States since 2002.

SWIFT data will be transmitted to third countries. Only information derived from terrorism, investigations (so called "lead information") could be transferred to third country counter terrorism authorities.

The envisaged agreement shall be based on Articles 216, Articles 82 (judicial cooperation) and 87 (police cooperation) of the Treaty on the "Functioning of the European Union.

In line with Article 218 of the TFEU, the Commission shall be nominated as the Union negotiator.

In line with Article 218 of the TFEU the European Parliament shall be Immediately and fully informed at all stages of the procedure.
Bearing In mind that the TFTP represents a considerable value for EU security and in the context of the continuing threat from terrorism in the EU, the Commission recommends to the Council to authorize the opening of negotiations with the United States of America regarding an international agreement (hereinafter "the Agreement") to require the making available on the basis of a push system to the United States of relevant financial messaging data which are necessary for the exclusive purpose of the fight against terrorism and its financing. The Agreement shall contain the necessary provisions to ensure that contracting parties respect EU data protection principles in all processing of personal data contained in financial messaging data made available to the U.S. pursuant to the Agreement.

RECOMMENDATION

In light of the above considerations, the Commission recommends:

- that the Council authorizes the Commission to negotiate on behalf of the European Union with the United States of America with a view to concluding a bilateral Agreement on the processing of Financial Messaging Data for purposes of the Terrorist Finance Tracking Program;
- that the Council issues the appended negotiating directives;
- that the Council designates a special committee to assist the Commission in its negotiating task.

ANNEX NEGOTIATING DIRECTIVES

The Agreement shall apply only to specific, designated providers of international financial payment messaging services ("Providers") as set out in the Agreement and/or its Annex for purposes of the Agreement;

The Agreement or its Annex shall provide that all transactions relating to the Single European Payment Area (SEPA) fall outside the scope of the data to be requested by or made available to the 'US Treasury Department, whichever system of financial messaging will be used;

The Agreement shall further provide that a judicial public authority ("the Authority") shall be designated in the EU with the responsibility to receive requests from the United States Department of the Treasury. The request shall indicate as specifically as possible the financial payment messaging data. On receipt of such requests, the Authority shall verify whether the substantiated request meets the requirements of the Agreement. As appropriate the Authority shall require the Provider to transfer, on the basis of a "push" system, the relevant financial payment messaging and related data;

The designated "Providers", "the Authority", as well as the scope of the financial payment messaging and related data to be covered shall be further specified in the Agreement and/or its Annex;

This Agreement shall provide that the request and the data, which is made available, shall take account of past and current analyses focused on message types and geography as well as perceived threats and vulnerabilities. The request as appropriate, shall be narrowly tailored, proportionate and clearly substantiate the necessity of the requested data. Only the minimum amount of data, which is necessary for the purpose of the Agreement, shall be requested by the United States Department of the Treasury. If need be the parties shall consult. The data, shall then be made available to the United States Department of the Treasury;

The Agreement shall limit the processing of personal data contained in relevant financial payment messaging data exclusively to the investigation, prevention, detection or prosecution, of terrorism and its financing as based on the approach of Article I of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism;

The Agreement shall ensure full respect for fundamental rights as enshrined-in Article 6 of the Treaty on European Union, in particular the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union. It shall also ensure full respect for the principles of necessity and proportionality regarding the right for private and family life and the protection of personal data as set out in Article 8 of the European Convention, on Human Rights and Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union;

The Agreement shall ensure rights of effective administrative and judicial redress on a non-discriminatory basis regardless of nationality for any person whose data are processed pursuant to this Agreement, in line with Article 47 of the Charter of Fundamental Rights of the European Union;

The Agreement shall contain safeguards and controls which ensure an adequate level of protection of personal data;

The Agreement shall ensure that personal data extracted from the TFTP database are kept for no longer than necessary for the specific investigation or prosecution for which they are accessed under the TFTP. As regards non-

extracted data the Agreement shall establish a maximum storage period of five years and provide for an ongoing and at least annual evaluation in order to identify and delete at the earliest possible stage all non-extracted data that are not necessary for the execution of the purposes referred to in the Agreement.

Onward transfer of information obtained through the TFTP under the Agreement shall be limited to law enforcement, public security, or counter terrorism authorities of US government agencies or of EU Member States and third countries or Europol or Eurojust as well as Interpol. No personal data shall be shared other than that contained in specific lead information on identified terrorism suspects. Such information shall be used exclusively for the investigation, detection, prevention, or prosecution of terrorism or its financing. Each onward transfer shall be duly logged.

The Agreement shall provide for:
1) the right of individuals to information relating to the processing of personal data;
2) the right to access his/her personal data;
3) to the rectification, and
4) as appropriate erasure thereof.

The Agreement shall provide for the right of any person to obtain, following requests made at reasonable intervals, without constraint and without excessive delay or expense, at least a confirmation via his/her national data protection supervisory authority as to whether their rights as a data subject have been respected. It will clearly lay down the eventual limitations to the exercise of the right to access, rectification and erasure, that may be set out to safeguard the prevention, investigation, detection and prosecution of terrorism or its financing covered by this Agreement based on the principles of necessity and proportionality. Any refusal or restriction to access shall be set out in writing to the data subject, and information shall be provided on the means available for seeking redress in the United States. In all of these cases the data subject shall be advised that he/she may appeal to a judicial authority;

The Agreement shall prohibit that financial payment messaging data transferred to the United States Department of the Treasury are subject to data mining, manipulation or otherwise interconnected with other databases;

The Agreement shall provide for safeguards and controls regarding the protection of personal data made available pursuant to the Agreement, including the monitoring of such safeguards and controls. Such safeguards and controls shall be at least equivalent to those for US citizens under US domestic law and as set out in the TFTP Representations. It shall reflect the standards set out in the Council of Europe Convention 108 of 8 November 2001;

The Agreement shall ensure that information, which is derived from the TFTP which, may contribute to the investigation, prevention, detection or prosecution of terrorism or its financing by one or more European Union Member States shall be made available in the most expedient manner to competent authorities of the

European Union Member States as well as to Europe and Eurojust. The Agreement shall further provide that appropriate searches of the TFTP database shall be carried out in response to a request made by the competent authorities of one or more European Union Member States, Europol or Eurojust and that these shall be provided with relevant extracted Information under the conditions of the Agreement;

The Agreement shall provide for a commitment of the US to cooperate with the EU if the EU decides to establish a database on European territory throughout the term of the Agreement so that the transfer of data can be more targeted in the future. It shall, provide for a commitment of the US to cooperate with the EU if the EU decided to set up an EU TFTP throughout this time. It shall provide for a commitment that in the event of the European Union setting up an EU TFTP, competent US authorities shall agree to cooperate on a reciprocal basis;

To avoid any risk that the envisaged Agreement could be seen as a precedent for data transfers in other areas, the Agreement shall state that it is specific to the fight against terrorism which represents a common EU-US interest and that the Agreement in no way constitutes a precedent for data transfers for any other purpose, for transfers of any other data or for any future EU-US data protection arrangements;

The Agreement shall specify that the European Union shall carry out regular reviews of the safeguards, controls and reciprocity provisions contained in the Agreement. Such reviews shall include access to TFTP systems to verify compliance with surrounding safeguards and controls. The reviews shall include a proportionality assessment of the retained data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing. The reviews shall include an assessment concerning the quantity of financial messages processed and the extent to which these data have been shared with other US agencies and/or third countries or Interpol. The review team shall include counter terrorism as well as data protection specialists;

The Agreement shall provide that the Commission will present periodical reports to the European Parliament and the Council on the functioning of the Agreement. The report shall indicate, in particular.
1) the quantity of financial messages processed,
2) the extent to which these data have been shared with other US agencies, public authorities of EU Member States or third countries, Interpol, Europol and Eurojust.
3) the numbers of cases for which the information has been used for the investigation, prevention, detection, or prosecution of terrorism or its financing and
4) compliance with data protection obligations.

The report shall present an assessment of the implementation of the Agreement and of the elements that would affect the compliance with the provisions of the Agreement;

The Agreement shall provide for its termination by either party upon at least one (1) year written notice to the other party;

Moreover, the Agreement shall provide that the EU shall have the right to immediately terminate the Agreement or require suspension of the transfer of financial payment messaging data where safeguards on reciprocity or obligations are not complied with;

The Agreement shall specify that it in no way affects the data protection standards established by the relevant EU or national legislation applicable to the “Providers” nor limit the supervisory competence and powers of data protection authorities, which are competent for the supervision of data processing by the "Providers";

The Agreement shall be equally authentic in the Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish language and shall include a language clause to this effect;

The Agreement shall accommodate the opt-ins and opt-outs possibilities, which are provided by the Protocols attached to the Treaties.