



## GENERAL SECRETARIAT OF THE COUNCIL OF THE EU

### *~INFORMATION NOTE~*

# **EU-US agreement on the processing and transfer of financial messaging data for purposes of the US Terrorist Finance Tracking Programme (TFTP) - Questions and Answers -**

November 2009

#### **1. What is the Terrorist Finance Tracking Programme?**

Under the Terrorist Finance Tracking Programme (TFTP) the United States Department of the Treasury (U.S. Treasury Department) seeks to identify, track and pursue suspected terrorists and their providers of finance. As part of the TFTP the U.S. Treasury Department requires by law the U.S. arm of SWIFT to transfer to it identified sets of financial messaging data relevant to terrorism investigations. Requests for data are narrowly tailored based on past analyses of relevant message types, geography and perceived terrorism threats. General data sets are transferred to the Treasury Department under the TFTP. However these data are not subject to open-ended searching, but instead are subject to specific searches based on pre-existing information demonstrating a reason to believe that the subject of the search is connected to terrorism or its financing. Data not subject to a specific search are and remain anonymous.

#### **2. Is the TFTP important for European security?**

More than 1450 TFTP-generated leads have been passed to date to European governments and 800 have been passed to non-European governments, with over 100 new TFTP-generated leads provided to EU countries from January to September 2009. Concrete examples of the benefits of TFTP-derived information include:

## **P R E S S E**

- (i) TFTP information provided substantial assistance to European governments during investigations into the Al-Qa'ida-directed plot to attack transatlantic airline flights travelling between the EU and the United States. TFTP information provided new leads, corroborated identities and revealed relationships among individuals responsible for this terrorist plot. In mid-September 2009 three individuals were convicted in the UK, and each was sentenced to at least 30 years in prison;
- (ii) In early 2009 TFTP was used to identify financial activity of a Europe-based Al-Qa'ida individual who played a role in the planning of an alleged attack on aircraft. The information was passed to the governments of European and Middle Eastern countries;
- (iii) In summer 2007 the TFTP was used to identify financial activities of members of the Islamic Jihad Union (IJU) in Germany. This information contributed to the investigation and eventual arrest of IJU members plotting to attack sites in Germany. The TFTP continued to provide additional useful information to German authorities following the arrests. The persons subsequently confessed.

### **3. What is the background of the Terrorist Finance Tracking Programme?**

The TFTP has existed for eight years. It was set up by the United States Department of the Treasury shortly after the terrorist attacks of 11 September 2001. The TFTP is based on U.S. statutory authorities, a series of UN Security Council Resolutions and related executive orders. A series of press articles in 2006 revealed the existence of the TFTP and led to concerns being raised in the EU about data protection. To address these concerns, the German Presidency of the EU (first semester 2007) supported by the Commission, negotiated a set of undertakings with the U.S. Treasury Department concerning how EU-originating personal data would be processed under the TFTP. These undertakings were published in the Official Journal of the European Union in July 2007 [C 166/18 of 20.7.2007].

### **4. What were the main data protection commitments that the U.S. Treasury Department made in the TFTP Representations?**

The U.S. Treasury Department Representations of July 2007 explained that data received under the TFTP had been and would continue to be used exclusively for the fight against terrorism. Use of the data for any other purpose, including any criminal or other activity not connected to terrorism, is strictly prohibited. The Treasury Department stated that any form of data mining of TFTP data has been and would continue to be strictly forbidden – under the TFTP data can only be accessed for a specific search by a counter terrorism analyst based on pre-existing information demonstrating a reason to believe that an identified person is engaged in terrorism or its financing. The Treasury Department undertook to delete data within a specified period – generally within five years, which is in keeping with EU law on anti-terrorist financing which requires banks in the EU to keep financial transaction records for five years.

**5. The TFTP Representations allowed the EU to designate an "eminent European person" to verify that the U.S. is respecting the commitments made in its undertakings. What did the "eminent European person" conclude?**

In early 2008 the European Commission designated the French counter terrorism judge Mr. Jean-Louis Bruguière for this purpose. Judge Bruguière produced a report in December 2008 with two main conclusions. First he confirmed the accuracy of the U.S. Treasury Department's representations to the EU with respect to data protection practices. Second, he concluded that the TFTP has generated significant security benefits for the EU. In the latter regard Judge Bruguière reported that TFTP leads shared with EU authorities have not only been extremely valuable in investigating terrorist attacks which have taken place in Europe over the last eight years, but have also been instrumental in *preventing* a number of terrorist attacks in Europe.

**6. If the TFTP has been operating for the last eight years, why is the EU proposing to enter into an agreement with the United States now?**

By the end of 2009, SWIFT will implement its new "systems architecture". For this purpose SWIFT will retain its existing EU-based and U.S. servers and will bring into operation a new operating centre in Switzerland. The net effect of this new arrangement is that a significant volume of the data which are currently received by the U.S. Treasury Department under the TFTP will no longer be stored in the United States. In order to ensure that the TFTP continues to produce the above-mentioned EU - and wider global – security benefits, it is necessary to put in place an international agreement that allows for data needed for the TFTP to continue to be made available to the U.S. Treasury Department. This is why in July of this year the 27 Member States of the European Union unanimously gave the EU Presidency a mandate to negotiate an agreement with the United States to ensure the transfer of the data and thereby the continuation of the TFTP. In July, it was not known when or indeed whether the Lisbon Treaty would come into force. Accordingly, the mandate is based on the legal mechanism of the EU Treaty which will cease to exist on 1 December when the Lisbon Treaty enters into force. To ensure that the European Parliament is able to exercise its new powers under the new Treaty in this regard, the envisaged Agreement is for a maximum duration of 9 months. The Commission will come forward with a new proposed mandate in early 2010 for a subsequent agreement based on the Lisbon Treaty. In the meantime, an interim agreement is needed to ensure that there is no lapse in TFTP coverage that would deprive the EU of important information related to terrorist attacks or investigations.

**7. Does the proposed EU-US Agreement improve the protection afforded to EU citizens by comparison with the current situation?**

In the TFTP Representations of July 2007, the U.S. Treasury Department made a number of unilateral commitments to the European Union about how it would process EU-originating data. Under the envisaged EU-U.S. Agreement, these unilateral commitments will become legally binding obligations in an international agreement. Breach of these obligations, for example, would entitle the EU to suspend or terminate the Agreement. Under the proposed Agreement the decision to authorise transfer of data to the U.S. Treasury Department will be made by a European judicial authority which must verify the legality of the request. This is a significant shift from the current situation where requests to transfer data are made directly to a private organisation without oversight by a European public authority.

**8. In what other respects does the proposed EU-U.S. agreement improve matters by comparison with the current situation?**

The envisaged Agreement provides for reviews of the way the TFTP is operating so as to assess in particular compliance with the data protection safeguards. Either party can request a review at any stage; in any event a review must take place within six months from the date of the Agreement. The review team will comprise representatives of the EU Presidency, the European Commission and Member States' Data Protection Authorities. The envisaged Agreement also seeks to strengthen the security benefits of the TFTP for the EU. For example, it *obliges* U.S. authorities to share with their EU counterparts TFTP leads obtained by the U.S. which are likely to be of benefit in the fight against terrorism in the EU. The Agreement will also allow Member State authorities to request a search of TFTP data where they have reason to believe that a person is engaged in terrorism or its financing.

**9. Will the U.S Treasury Department receive more data under the proposed agreement than under the current arrangement?**

The Agreement seeks to ensure the sustainability of the TFTP as it currently exists. The Agreement does not foresee the transfer of any additional types of data.

**10. What safeguards does the proposed EU-US Agreement contain for the protection of personal data?**

The Agreement contains significant safeguards for the protection of personal data transferred under the Agreement. These include, for example, a strict prohibition on using the data for any purpose other than the prevention, investigation, detection or prosecution of terrorism or its financing, including the specific demonstration of a "reason to believe" that the subject of a search is connected to terrorism. The Agreement prohibits any form of data mining. The Agreement requires the Treasury Department to identify data which are no longer needed for counter-terrorism purposes and to delete them. In other cases, data held on the TFTP database generally must be deleted within five years from receipt. The Agreement imposes strict obligations on data security and on the persons entitled to access TFTP data.

**11. How can individuals be sure that their personal data has not been processed incorrect?**

The existing rights of individuals or data protection authorities within the EU are not infringed. Any person has the right to obtain confirmation from his or her data protection authority whether all necessary verifications have taken place within the European Union. Any person can make such requests at reasonable intervals, without constraint and without excessive delay or expense. It should be noted that such right may be subject to necessary and proportionate limitations applicable under national law, including for the protection of public security or to avoid prejudicing criminal investigations, with due regard for the legitimate interest of the person concerned.

**12. What rights of redress will an EU citizen have if his or her data are processed in breach of the safeguards set out in the Agreement?**

The Agreement states that any person whose personal data are mishandled in breach of the Agreement is entitled to seek effective legal redress. Under U.S. law for example, the Administrative Procedure Act allows a person who has suffered harm as a result of governmental action to seek judicial review of the action. Also under U.S. law the Inspector General Act would allow, for example, the Inspector General of the U.S. Treasury Department to investigate complaints concerning abuses or deficiencies relating to the administration of the TFTP and to report their findings to the Treasury Secretary and to Congress.

**13. What kinds of data are transferred to the U.S. Treasury Department under the TFTP?**

The data transferred under the TFTP are completed financial transaction record data. Such data may include identifying information about the originator and/or recipient of the transaction, including name, address, national identification number and other personal data related to financial messages.

**14. Why is the Agreement stated to be for a maximum duration of 9 months?**

The envisaged Agreement has a short duration in order to ensure that the European Parliament's new powers under the Lisbon Treaty will apply to any possible longer term agreement which might replace the envisaged Agreement.

**15. In September 2009 the European Parliament adopted a Resolution on the envisaged EU-U.S. Agreement. Is the proposed Agreement in line with the Resolution?**

The envisaged Agreement is very much in line with the conditions set by the Resolution. For example, the agreement has a maximum duration of 9 months; a more long term agreement will be based on the Lisbon Treaty. Substantive conditions of the Resolution are also met or enhanced. For example, the Resolution calls for requests of data to be based on specific targeted cases and to be subject to judicial authorisation; the Agreement to prohibit any use of financial messaging data for purposes other than the fight against terrorism; and the Agreement to include a reciprocity mechanism to ensure that Member State services receive TFTP-derived information upon request.

---