Comments on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 13 July 2011: "A European terrorist finance tracking system: Available options"

1. *General context and origin of the scheme*

The Communication recalls that the main reason for the development of a European terrorist finance tracking system ('EU TFTS') has its source in the present US TFTP agreement (and in particular its Article 11) and in the Council Decision of 13 July 2010 ('the Decision'). Currently, under TFTP, data are sent in bulk to the US, to be stored and filtered according to requests of the US Treasury Department. This has raised serious criticism, especially by the European Parliament (and obviously the EDPS and WP29), notably with regard to the necessity and proportionality of the 'bulk' data flows.

The agreement envisages a possible "*cooperation with a future equivalent EU system*" in case the Commission, following an own study, would decide to establish an EU system "*allowing for a more targeted transfer of data*".

In the Decision, the Council agreed to the conclusion of the agreement between the EU and the US while at the same time inviting the Commission to submit to the European Parliament and to the Council a legal and technical framework for the extraction of data on EU territory. Furthermore, in giving its approval to the conclusion of the agreement on 8 July 2010, the European Parliament explicitly acknowledged the commitment by the Council and the Commission to set up the legal and technical framework allowing for the *extraction of data* on EU soil. This commitment would in the mid-term ensure the termination of bulk data transfers to the US authorities.

The requirement for a prior filtering of data within the EU is supported by the EDPS, as it would prevent the sending of bulk data to a third country. However, the Communication goes beyond the acknowledged purpose of filtering data in the EU, as it clearly indicates that the "*system should not be set up just to provide relevant information to US authorities*", as the authorities of the Member States "*have a real interest in the results of such a system as well*"[1].

The Communication therefore seems to legitimise the setting up of a whole new TFTS scheme, in an EU specific context, on the basis of the existing TFTP agreement. In other words, the Communication seems to justify the introduction of a new system which invades the privacy of EU citizens for the benefit of the authorities of EU Member States while using as a justification the assessment of utility of a system conceived and implemented to allow the US authorities to pursue their own investigation linked to terrorism.

The EDPS has strong doubts about this approach, which does not appear to respect the principles of necessity and proportionality (as developed below).

[1] Communication, paragraph 3, p. 4.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. *Necessity and proportionality*

Necessity

The Communication mentions on several occasions the “added value” or the “interest” of the US TFTP, without referring to any analysis of the efficiency of existing tools, including Financial Intelligence Units (FIUs) which already have a specific role in relation to the financing of terrorism, as they collaborate within the so called Egmont Group to exchange financial intelligence data.

A positive assessment of the US TFTP, which allegedly seems to satisfy the needs of the US authorities, cannot be transposed as such to the internal EU framework, without analysing thoroughly the existing instruments available to the EU investigative authorities and – in case these existing instruments are not fully satisfactory - the possible needs for a new scheme in the specific EU context.

The EDPS strongly recommends that such an in-depth analysis is conducted in the context of the Impact Assessment. This analysis should first and foremost concentrate on the conditions and safeguards necessary for the setting up of a filtering system within the EU, in the context of the TFTP agreement with the US. It is only in a second stage that any need for an EU TFTS scheme should be analysed, taking account of the mechanisms which already exist based on the current EU framework.

The EDPS has advocated the need for an assessment of all existing instruments in the area of freedom, security and justice before proposing new ones in numerous opinions and comments[2]. Evaluating the effectiveness of existing measures while considering the impact on privacy of new envisaged measures is crucial and should play an essential role in the European Union's action in this area, in line with the approach put forward by the Stockholm Program

Proportionality

As stated above, the main proportionality issue currently affecting the TFTP consists of the collection of data in bulk by the US authorities at the source of the processing, i.e. at the financial transfer company on European soil. The US TFTP is said to be based on a robust and well developed data protection framework (as stated on p.5 of the Communication) as well as on the limitation of purpose to combating terrorism and its financing (see p.3 of the Communication). However, these elements as such do not “compensate for the provision of bulk data”, as alleged in the Communication (p.3). They do not meet the preliminary requirements of proportionality as developed above.

Given this serious shortcoming of the current TFTP, the Commission should not rely on the proportionality analysis made in the context of TFTP. The EDPS therefore strongly recommends that an in-depth, independent proportionality analysis be carried out in relation to the proposed TFTS in the Impact Assessment. It should address the way in which the extraction of data on EU territory is envisaged, in particular how and which data are supposed to be transferred from the financial transfer company to the authority that is supposed to carry

[2] See for instance Opinion on the "Overview of information management in the area of freedom, security and justice", 22 June 2010 and Opinion on the Communication from the Commission to the European Parliament and the Council - "The EU Counter-Terrorism Policy: main achievements and future challenges", 24 November 2010.

out the investigation. The assessment must evaluate ways to minimize processing of personal data in this context. The Impact Assessment should also, separately, address the proportionality of creating a new European TFTS in relation to the objective of fighting the financing of terrorism, as acknowledged in the Communication (p.3).

3. Procedural guarantees

The EDPS would also like to highlight the lack of sufficient clarity on the procedural guarantees envisaged in the three options for TFTS described by the Communication. The Communication distinguishes various functions that need to be carried out in order to implement the tracking of terrorist financing.

The first step is the preparation and issuance of the 'requests' by the authorities to the designated providers of financial messaging services for the raw data. These requests must then be monitored and authorised. In the Communication, the Commission considers two options regarding the origin of requests: either they would come from an 'EU central TFTS unit' (option 1 and 2), or from the 'upgraded FIU coordination service' (option 3). The terminology used to indicate what kind of procedural guarantees are to be applied in the "request" phase in the three options remains however vague. The EDPS calls on the Commission to develop specific and strong guarantees.

This aspect is all the more important as it constitutes a fundamental difference with the current US TFTP system. While in the latter system the requests (production orders) originate from the US Treasury Department and must respect the criteria established in Article 4 of the agreement (specificity of the request, necessity, narrow tailoring, exclusion of SEPA data), in the three options considered by the Communication there is no trace of the substantial criteria (which level of suspicion, existence of other proof, etc…) on the basis of which any request for data extraction should be initially verified.

For instance, the text of the Communication mentions that the requests for option (1) "*could take place in consultation with the responsible authorities of the Member States*", that Member States would need to "*share information*" with the EU central TFTS to substantiate the request and its nexus to terrorism, or have the requests "*pre-authorised*" by national authorities. It is then mentioned that such authorities could be for example national counter-terrorism prosecutors or investigation judges. In this case no further intelligence would be required from the EU central TFTS unit.

In this scenario there is no indication of which substantial or procedural elements must be assessed before any type of search is authorized. The fact that pre-authorisation by judicial authorities – which presumably are involved in investigations on terrorism - is referred to as only one of the possibilities considered by option 1 raises a fundamental issue: the EDPS has strong doubts as to whether any request related to an investigation on terrorism could be justified otherwise than under the control of the judiciary authorities. Any request would entail a serious interference with the protection of personal data of EU citizens who do not have any connection with terrorist activities; therefore it must be stressed that such interference should only be allowed upon approval of the judicial authorities of the various Member States on the basis of substantial criteria.

As highlighted above, the Communication remains vague in this respect. The EDPS therefore urges the Commission to clarify, especially in the context of an EU centralized coordination and analytical service, which substantial criteria must be respected in order to initially issue

the requests, and to reflect upon the importance of the procedural guarantees offered by the national criminal procedural laws established in the various Member States.

Also the role of the FIUs in the proposed upgraded "FIU platform" (option 3 of the Communication) should be clarified, and compared to the present competences of the FIUs. For the same reasons mentioned above, clear conditions of collaboration with the judiciary should be analyzed and substantiated in order to ensure the respect of procedural guarantees established in the judicial systems of the various Member States.

4. Oversight mechanisms

With regard to oversight mechanisms, the Communication also mentions the possible role of "overseers". It is unclear to what extent the role of these overseers would be defined in analogy with their role in the US TFTP agreement, and if oversight by private actors is envisaged. We consider that such a mechanism involving private actors should not be transposed to the EU framework. The EU framework requires institutionalised supervision and any specific role given to overseers should in no event replace the judicial guarantees mentioned above and the oversight role of data protection authorities.

5. Use of existing structures

The Communication supports the use of structures which already exist (p. 6). This raises issues of interoperability and risks of function creep. The fact that an existing structure is used should not allow exchange of data with other databases. It must be recalled that no interconnection of databases should be established without a clear and legitimate basis[3]. Besides, personal data should not be used for purposes deviating from those strictly defined in the scheme, which in the view of the EDPS should be strictly limited to the fight against terrorism and its financing: the use of an existing structure does not ensure *per se* compliance with the principle of purpose limitation.

Consequences of a possible EU TFTS in relation to the existing US TFTP

The US TFTP has been developed by US authorities in order to obtain access in a more speedy and efficient way to financial data, rather than going through the procedure foreseen in existing instruments, notably the agreement on mutual legal assistance between the EU and the US[4] and the measures set up by the Financial Action Task Force (FATF), involving national FIUs. US TFTP allows US authorities to access a broader range of data, and perform searches themselves based on their own criteria. This is one of the main data protection issues, as the proportionality test is not met according to EU standards, as developed in previous opinions of the EDPS and the Article 29 Working Party[5].

---

[3] See in this respect the Comments of the EDPS of 10 March 2006 on the Communication of the Commission on interoperability of European databases, available at www.edps.europa.eu: *Interoperability is mentioned not only in relation to the common use of large scale IT systems, but also with regard to possibilities of accessing or exchanging data, or even of merging databases. This is regrettable since different kinds of interoperability require different safeguards and conditions. This is for instance the case when the concept of interoperability is used as a platform of other proposed measures aiming to facilitate the exchange of information. The EDPS opinion on the principle of availability emphasised that although the introduction of this principle will not lead to new databases, it will necessarily introduce a new use of existing data bases by providing new possibilities of access to those data bases.*

[4] Council Decision of 6 June 2003 concerning the signature of the Agreements between the European Union and the United States of America on extradition and mutual legal assistance in criminal matters; OJ L181 of 19/07/2003, p.25

[5] See in particular:

If the filtering of data is performed within the EU under TFTS, according to criteria which should be particularly strict (in order to comply with the necessity and proportionality tests), the data sent to the US would be restricted as a result. This is essential in order to meet the EU data protection requirements, even if the data would not totally meet the (broad) requests of US authorities.

The impact of this change on the overall rationale of the US TFTP agreement is not examined by the Communication, although this specific point is raised in Article 12(3) of the agreement itself. The EDPS invites the Commission to reflect upon the actual impact that an EU TFTS would have on the current implementation of the US TFTP. The Commission should verify whether an earlier review of the agreement is necessary in order to adapt the rules governing the EU-US transfer of financial messaging data to the envisaged new system.

The EDPS looks forward to such an in depth analysis in the Impact Assessment now being prepared by the Commission, on which he should be consulted.

Brussels, 25 October 2011

- EDPS Opinion of 22 June 2010 on the Proposal for a Council Decision on the conclusion of the 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 (TFTP II), available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-06-22_Opinion_TFTP_EN.pdf
- Opinion 10/2006 of the Article 29 Working Party on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf