



CONSEIL DE
L'UNION EUROPÉENNE

Brussels, 2 September 2011

13716/11

LIMITE

JAI 579
ECOFIN 557
DATAPROTECT 86
ENFOPOL 275

Translation provided by French Delegation

NOTE

from:	the French delegation
to:	CATS
No. prev. doc.	12957/11 GENVAL 81 JAI 522 ECOFIN 523 DATAPROTECT 75 ENFOPOL 245
Subject:	France's position with respect to a European TFTP

The EU/USA Agreement "*on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*" (TFTP) was signed on 28 June 2010 and was the subject of a Council Decision on 13 July 2010. Article 11 of the Agreement states that "*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*". On 13 July 2011, the Commission presented a communication¹ about the available options for a European terrorist finance tracking system.

¹ 12957/11 GENVAL 81 JAI 522 ECOFIN 523 DATAPROTECT 75 ENFOPOL 245.

France is in favour of the creation of a European TFTP. Such a programme would give Member States – in accordance with European law and under conditions to be defined based on domestic legislation – access to a tool that has, for the US and its partners, proved to be indispensable in preventing and combating terrorism.

The goal of this note is to indicate France's view of the principles that should guide the creation of such a system. In this respect, we would like introduce four initial considerations:

- 1) The structure of any future system should comply fully with the provisions of Article 72 of the TFEU, i.e. with the prerogatives of Member States with regard to the maintenance of law and order and the safeguarding of internal security. This category includes the preventive aspect of the fight against terrorism, which is a major goal of the Member States.
- 2) Given the project's complexity, it is important, whenever possible, to make use of existing EU structures, in particular to avoid legislation over and above the adoption of the TFTP regulation. For this reason in particular, France proposes involving the Financial Intelligence Units, which also offer high levels of guarantee with respect to data use and protection. France, as it emphasized throughout the negotiation of the EU/USA Agreement, is aware that the TFTP would involve large-scale transfers of data.
- 3) The effectiveness of the program also means complying with operational principles shared by all Member States with respect to the fight against terrorism: these principles are based on secrecy or, at the very least, on a high level of confidentiality.

4) Overall, the programme should be designed to be compatible with the system implemented with the US. On the one hand, the United States has agreed, in the aforementioned Agreement, to a technology transfer, which will help reduce design costs of the system. On the other hand – again under the terms of the Agreement – the United States and the European Union have agreed, once the European system is operational, to cooperate via their respective TFTP.

The following proposals are thus based on the various phases as perceived in the American TFTP. They correspond to four distinct tasks, three of which can be carried out at EU level.

1) First business: selecting messages to populate the database

In order to create a searchable database, the American system presupposes the large-scale transfer of financial messages from the financial messaging provider to the Treasury Department. Only those messages that are relevant to the fight against terrorism are selected and placed in the database.

The selection process, which involves terrorist threat identification skills, has a threefold importance:

- It limits the size of both the transfer and the data storage facilities, which is important when it comes to data protection;
- It makes searching more effective;
- By limiting the size of the database, it also keeps costs down.

France's view is that data requests made to the financial messaging provider should be made by an ad hoc authority based on requests from Member States, thanks to the legal basis supplied by the regulation setting up the TFTP. The mission of this authority will be similar to that carried out by the US Treasury Department within the context of the American TFTP.

To allow it to carry out its missions, the organization of this authority will have to be defined. It could be set up along the lines of the "FIU Platform", whose existence and operation should be made official on this occasion.

2) Second business : developing and managing the database

The messages selected in compliance with point 1 will be placed in a database for later use (point 3). France believes that the future Agency for the Operational Management of Large-Scale IT Systems in the area of Freedom, Security and Justice¹, which should be operational by 2012, is the suitable structure to accomplish this. The development and operational management of large-scale IT systems is the first mission with which it will be tasked². As it will do for the other systems for which it will be responsible (SIS II, Eurodac, VIS and others), the agency will confine itself to providing technical support in order to access the data, under the conditions described in the following point. By so doing, the EU will be using the same method used for SIS II, VIS and EURODAC – European-level management of a system that benefits all Member States.

3) Third business : processing and analyzing data

Operational processing of data for the purposes of analysis falls within the purview of the Member States, given their mission to prevent and combat terrorism and given that they are the only ones with upstream access to information for carrying out such an analysis. In addition, only Member States are in a position to act in a situation where analysis of data in the TFTP could uncover a terrorist plan.

¹ COM (2009) 293 final.

² See Article 1 of the draft Regulation.

France also believes that if the new infrastructure is to make the same database search tool available to all Member States, it must also allow any Member States that so desire to develop their own tools, providing they authorise the monitoring called for in point 4.

The system thus defined – one in complete compliance with the principles governing the fight against terrorism – is the only one that is acceptable to France.

The system may come under fire for not encouraging data sharing at a European level. It should be pointed out that the TFTP will not change the rules applicable within the EU in terms of the fight against terrorism. Above all, France proposes that the national authorities with the competence to operate the database should be the FIUs, as defined in AML/CTF legislation, the creation of which is mandatory under EU law¹. Minimum standards of quality to be met by compatible FIUs with access to the database should be defined. In accordance with Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, these Units already have their own communication mechanism allowing them to exchange data in a manner adapted to the type of information to which the TFTP provides access². Finally, the FIUs may work together with FIUs in third countries.

Within a restricted framework defined by the Agreement, the *ad hoc* authority mentioned above (see point 1) could nevertheless be granted an access to the database that is independent of the Member States' national authorities to allow data searches requested by the United States.

¹ JO L 309, 25.11.2005.

² JO L 271, 24.10.2000.

4) Fourth business : monitoring data use

France believes that, on the basis of EU regulations, that a data protection scheme should be put in place that is adapted to the nature of the system, and one that will ensure that data use is strictly confined to the purposes for which it was intended. Such a scheme should be based on the one put in place for the American TFTP. For this reason, a shared monitoring mechanism should be put in place at the European level, independent of the one called for within the context of message selection. It must provide guarantees of both independence and neutrality, within the context of strict confidentiality. In particular, it must include, like the American system, independent analysts with the authority to block, on a 24-hour basis, requests that do not appear to be in line with the goals of the TFTP, and to carry out retrospective monitoring of the entire structure. In addition, a data monitoring authority should be set up, or attached as the case may be, to an existing shared monitoring authority, such as FIU Platform. It will be also be responsible for complying with the data protection scheme, which, given the specific nature of this system, should be defined by the legislation setting up the European TFTP, on the basis of the rules applicable within the European Union.