004393/EU XXV. GP
Eingelangt am 29/11/13

COUNCIL OF THE EUROPEAN UNION

Brussels, 29 November 2013

17063/13

JAI 1092
DATAPROTECT 187
ECOFIN 1091
GENVAL 85
ENFOPOL 398

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	28 November 2013
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	COM(2013) 842 final
Subject:	Communication from the Commission to the European Parliament and the Council A European terrorist finance tracking system (EU TFTS)

Delegations will find attached Commission document COM(2013) 842 final.

_____

Encl.: COM(2013) 842 final

EUROPEAN
COMMISSION

Brussels, 27.11.2013
COM(2013) 842 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

A European terrorist finance tracking system (EU TFTS)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

A European terrorist finance tracking system (EU TFTS)

Following up the Communication of 13 July 2011 (COM (2011) 429) the aim of this Communication is to inform the European Parliament and the Council of the outcome of the analysis made with regard to the feasibility of the establishment of European Finance Tracking System (EU TFTS).

1. CONTEXT

1.1. Origin of the Request and definition

During the negotiations preceding the conclusion of the EU-US TFTP Agreeement[1], discussions took place on how best to protect personal data and respect fundamental rights in the context of this Agreement. It was argued by some parties that extracting data on European soil would limit the amount of data transferred to the U.S. and would therefore ensure a higher level of data protection guarantees. Some Member States saw an added value in developing an independent European system for tracking terrorist finance in the longer term. The European Parliament asked the Council and the Commission to take all measures necessary to devise a durable, legally sound European solution to the issue of the extraction of requested data on European soil. The Council and the European Parliament, when agreeing to the EU-US TFTP, invited the Commission to submit, within one year of the date of entry into force of the Agreement, a legal and technical framework for extraction of data on EU territory and, within three years of the date of entry into force of the Agreement, to present a progress report on the development of an equivalent EU system[2]. Furthermore, Article 11 of the EU-US TFTP Agreement states that during the course of the Agreement, the Commission will carry out a study into the possible introduction of an equivalent EU system allowing for a more targeted transfer of data.

For the purpose of this Communication an equivalent EU system should be distinguished from a framework for extraction of data on EU territory. A *framework for extraction of data* on EU territory is understood to be a system allowing searches on the data currently provided

[1] OJ L 195, 27.7.2010, p.5
[2] Council Decision of 13 July 2010, OJ L 195, 27.7.2010, p.3

by the EU to the U.S., to be conducted on EU soil. By contrast, *an equivalent EU system* would be an independent European system for tracking terrorist finance through access to, searches on and analysis of the data of Designated Provider(s). The establishment of any EU system would require a modification of the EU-US TFTP Agreement.

1.2. Steps taken

In December 2010 the Commission contracted *a study* which was extended in July 2011 to cover the additional option of a retention and extraction regime. In the course of this study the Commision held four expert meetings involving stakeholders such as Europol, the European Data Protection Supervisor, the TFTP Designated Provider[3] and many Member States' experts, representing interested ministries, law enforcement and intelligence agencies, and Data Protection Authorities.

On 13 July 2011 the Commission, in its *Communication to the European Parliament and the Council ('2011 Communication')* presented five possible options it had identified for an European terrorist finance tracking system ('EU TFTS'). Of these, three were deemed to be feasible. The objective of the 2011 Communication was to trigger a debate on the way forward and to feed into the Impact Assessement to be undertaken.

The issue was presented in October 2011 in the JHA Council and in the European Parliament Civil Liberties Committee.

As Member States and the European Parliament did not express a clear preference for any of the options it was decided to look at all of them in Commission's Impact Assessment, and to elaborate on them by developing different sub-options. This Communication builds on the Impact Assessment[4].

[3] Society for Worldwide Interbank Financial Telecommunication (SWIFT)
[4] SWD 2013 (xx) of

2. COMMISSION'S CORE PRINCIPLES AND OPTIONS IDENTIFIED

2.1. Principles of the Information Management Strategy adopted under the Swedish Presidency

In its analysis on the proposed way forward the Commission takes into account the core principles set out in the 2009 Information Management Strategy[5] and later incorporated and further developed in the Commission Communications on the Overview of information management in the area of freedom, security and justice in 2010[6] and on the European Information Exchange Model in 2012[7] .

Paramount in this regard are the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness.

Safeguarding *fundamental rights* as enshrined in the Charter of Fundamental Rights of the European Union, particularly the right to privacy and personal data protection, is a primary concern for the Commission when developing new proposals that involve the processing of personal data in the field of internal security. Articles 7 and 8 of the Charter proclaim everyone's right to 'respect for his or her private and family life' and 'the protection of personal data concerning him or her'. Article 16 of the Treaty on the Functioning of the European Union, which is binding on Member States, Union institutions, agencies, and bodies, reaffirms everyone's right to 'the protection of personal data concerning them'. According to Article 52 of the Charter, subject to the principle of proportionality, limitations on the exercise of the rights and freedoms recognised by the Charter may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Interference with the right to privacy is considered *necessary* if it answers a pressing need, if it is proportionate to the aim pursued and if the reasons put forwards by the public authority to justify it are relevant and sufficient.

Although it is difficult to assess all the costs of terrorism in financial terms, the principle of *cost- effectiveness* remains. A *cost-effective* approach takes account of pre-existing solutions

[5] Council conclusions Council Conclusions of 30 November 2009 on an Information Management Strategy for EU internal security 16637/09
[6] COM (2010) 385 of 20 July 2010
[7] COM(2012) 735 of 7 December 2012

to minimise overlap and to maximise possible synergies. An assessement is required as to whether it may be possible to accomplish a proposal's objectives through better use of existing instruments.

2.2. Approach

In light of the principles referred to above the Commission has examined whether an EU TFTS would be necessary and proportionate with regard to its costs, benefits and its impact on fundamental rights, as compared to the current situation.

In terms of *benefits*, an EU system could increase the EU's and its Member States' capacities to access relevant data and could strengthen their analytical capacities to track and identify terrorists through financial transactions. As financial transactions can yield valuable intelligence that may be unavailable from other sources this tool would have a particular value for detection of terrorist activitity and players involved. Therefore, an EU TFTS could represent an additional intelligence and investigation tool in the fight against terrorism and in enhancing security in the EU, in particular if such a system were to cover multiple financial data providers and types of transactions. The benefits of an EU TFTS need to be balanced with the estimated costs of introduction and maintaining of such a system, including the financial burden for the EU, the Member States, and for Designated Providers of the data in question.

2.3. Presentation of the Options

A number of options for both *the framework for extraction of* data on EU territory and *the EU equivalent system* have been considered.

2.3.1. A framework for extraction of data on EU Territory

A framework for extraction of data on the EU territory could be implemented through a system of retention and extraction of data held by the Designated Provider by allowing direct access to data, which is currently provided to the U.S. under the TFTP. This direct access would be given to US analysts or experts mandated for that purpose.

Under this option, one possibility would be to retain data on the server of Designated Provider for a certain period of time and run searches directly on this server. However, the current Designated Provider under the EU-US TFTP Agreement has put in place strong data

protection and security measures which do not allow for the identification of persons mentioned in message data content and so its current database does not permit searches based on personal data. Therefore the creation of a separate database would be required.

Alternatively, data could be extracted and held at a different secure location in the EU. The U.S. analysts or experts authorised to run the searches could either be physically located at the premises of the Designated Provider or could have remote access to the data. In all cases, and regardless of the location of data, comprehensive and solid safeguards would have to be put in place and tailored to the particular set-up of the system.

2.3.2. An EU equivalent system

A range of options for an EU equivalent system (as outlined in the 2011 Communication) have been assessed, including a fully centralized system at the EU level, a decentralized system at Member States' level and three hybrid systems in which both the EU and Member States would play a role.

Under each option there are different possibilities regarding the scope of the EU system. There are choices to be made as to types of messages and Designated Providers which would be included. An EU equivalent system could stick to or go beyond the type of financial messages and Designated Provider currently covered by the EU-US TFTP Agreement.

- The option of a fully centralized system at the EU level would mean that a single EU body would perform all the key functions of the system: requesting extraction of data, storing data, searching, carrying out intelligence analysis, safeguarding and monitoring the system, and disseminating intelligence leads to Member States. This option is legally unsound as it would not respect Article 72 of the TFEU, which confirms that the primary responsibility for maintaining of law and order and the safeguarding of internal security lies with the Member States. Such a system would be neither feasible nor acceptable for Members States, as it would require the creation of some form of centralized intelligence capacity at EU level
- A fully decentralized system at Member States' level would mean that the system would be run by Member States' competent authorities, with no functions being performed at EU level. This would mean that data could be transferred to and

searched by all 28 Member States in parallel. This option would multiply data flows and have important cost implications.. It would also lead to an increased risk of inconsistent treatment of data, and the creation of uneven data protection mechanisms. Therefore this option is also not considered to be viable.

These two options have thus been excluded from a more detailed assessment.

The three remaining options for an EU equivalent system entail distributing the different functions between different organizations at the EU and national levels ('hybrid systems').

In all these hybrid systems, the data would have to be requested on an ongoing and iterative basis from the Designated Provider(s), extracted, and stored in a database in a secure location in the EU. The actual searches would be then run against this central database. Similarly for all the options, appropriate data protection safeguards would have to be set up.

- A) In the first hybrid system, the EU TFTS coordination and analytical service, an EU central unit would have to be created. This would be tasked with requesting data from the Designated Provider(s), running searches, analysing intelligence and distributing the results. The difference from a fully centralized system would be that the Member States would have direct access to the system and would be able to request searches to be run on their behalf by the central unit or by their own analysts.
- B) The second hybrid system, the EU TFTS extraction service, would also involve the creation of an EU central unit. However, in this option the EU body would run searches at the request of Member States and would disseminate results to Member States without analysing the intelligence. However, the EU body would be able to run its own searches and to analyze the result of these searches.
- C) In the last hybrid system, the Financial Intelligence Unit[8] ('FIU') coordination service, an ad-hoc EU platform would be created. This would not be a permanent body but rather a group of financial intelligence experts participating in meetings. The FIU platform could be possibly upgraded for this purpose. Each Member State would nominate one representative who would act on its behalf. This ad-hoc authority would compile the requests from FIU's of each Member State and issue requests for data

[8] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information

from Designated Provider(s) based on these Member State requests. Each Member State's representative would be responsible for running searches, carrying out analysis and managing results on behalf of its own Member State. It would then be up to Member States' competent authorities to make use of the intelligence leads and further disseminate them at national level.

2.3.3. Status quo: EU-US TFTP Agreement

At present the EU and the Member States can request searches to be run by the US under the EU-US TFTP Agreement governing 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').

The TFTP is a counter-terrorism tool developed by the U.S. in the aftermath of the terrorist atttacks on 9/11. It is based on searching the data provided by the Designated Provider, including the data transferred from the EU.

The EU-US TFTP Agreement regulates thoroughly the process of requesting the data by the U.S. authorities. Europol verifies that the requests for data received from the U.S. are in conformity with the Agreement and, in particular, that they are as narrrowly tailored as possible in order to minimize the volume of data that is transferred. Numerous provisions cover secure handling, storage and deletion of the data. Provided data are held in a secure physical environment and stored separately from any other data. The Agreement prescribes a retention period of five years and an obligation to evaluate regularly the need to retain the data. The independent overseers located in the U.S. include two overseers selected by the EU. They exert a continous control on the way the system is run and they have a possibility to check every search conducted by the U.S. Treasury Department to ensure that a subject of a search has a nexus to terrorism or its financing.

The Agreement also includes provisions on the rights of access to and rectification of personal data, and on redress procedures. The Agreement provides that any person who considers his or her personal data to have been processed in breach of the Agreement may seek effective administrative or judicial reddress in accordance with the laws of the EU, its Member states, and the United States, respectively. The Agreement provides for persons, regardless of

nationality or country of residence, to have available under U.S. law a process for seeking judicial redress from an adverse administrative action.

Relevant statutes for seeking redress from an adverse Treasury Department administrative action in connection with personal data received pursuant to the Agreement include the Administrative Procedure Act and the Freedom of Information act. The Administrative Procedure Act allows persons who have suffered harm as a result of U.S. Government action to seek judicial review of that action. The Freedom of Information Act allows persons to utilize administrative and judicial remedies to seek government records. The existing uniform procedures for access to and/or rectification, erasure or blocking of personal data, agreed between the Commission, the U.S. and the Article 29 Working Party, aim to facilitate the exercise of these rights by the EU citizens. The implementation of the Agreement and its safeguards and controls is subject to regular reviews under Article 13 of the Agreement. Two such reviews were carried out in 2011[9] and 2012[10], concluding that the Agreement had been properly implemented. A third review is foreseen for spring 2014. The Joint Report regarding the value of Provided Data prepared pursuant to Article 6 of the Agreement demonstrates the benefits of the TFTP in preventing and combatting terrorism and its financing and the use of the TFTP made by several Member States. The TFTP information and its accuracy enable the identification and tracking of terrorist and their support networks across the world. It sheds light on the existing financial structures of terrorist organisations and allows for the identification of new streams of financial support and the actors involved.

3. ASSESSMENT

When assessing whether or not to propose the establishment of an EU TFTS the Commission has to reconcile the different views and expectations regarding the level of ambition of an EU system. EU TFTS goals are viewed differently by various stakeholders and decision makers. The Commission examined possibilities and implications of both scenarios against the principles for development and implementation of new policy initiatives detailed earlier. In particular, each option has been weighed in terms of necessity, proportionality and cost effectiveness.

[9] SEC (2011) 438 of 30 March 2011
[10] SWD (2012) 454 of 14 December 2012

3.1. A framework for extraction of data on EU Territory

As described in section 2.3.1. the option of a retention and extraction regime would serve as a way to collect, store and run searches on data, which are currently transferred to the U.S. under the EU-US TFTP Agreement, on EU soil. Thus it would not generate additional intelligence benefits for the EU or the Member States, compared to the present situation. On the contrary, with the TFTP data stored in the U.S. and the EU, fragmentation of searches, which currently run against one set of TFTP data, may have a negative impact on the quality and number of intelligence leads and worsen the overall efficiency of the TFTP. It may also significantly slow down the process of analysis, as different consecutive searches on the TFTP data stored in two locations could be necessary to further follow up an intelligence lead. Speed is often essential in terrorist investigations.

The extraction of the data on European soil instead of in the U.S. would not guarantee better protection of personal data *per se*. Protection of access to data is key to ensuring proper handling of data, regardless of its location. To this end, a set of robust safeguards would need to be put in place which would guarantee the compliance of data processing and handling with the necessary requirements. The system would have to be equiped with a control function responsible for verifying the requests for searches and their justifications. The role of independent overseers would be crucial in ensuring that the data is used for the limited purposes defined in any establishing Agreement. Measures would have to be taken to prevent unauthorised access to or disclosures of the data such as a maintaining the data in a secure physical environment. Procedures for access to and rectification of personal data and relevant redress procedures would have to be built in. An external audit would have to be commissioned to ensure the correct functioning of the system.

Under the EU-US TFTP Agreement the U.S. does not have access to all data of the Designated Provider but only to the sets of data which the U.S. requested as approved by Europol on the basis of past and current terrorism risk analyses. Unless a similar mechanism of initial narrowing of data requests is put in place, allowing direct searches to be run on all data of the Designated Provider would further increase the data exposure and the impact on data protection rights. This would require significant remodeling of the way the Designated Provider works and how its data are stored. Currently the financial messages which are subject to the Agreement are kept in a form that does not allow idenfication of persons

mentioned in message data content. Each financial message is encrypted and searchable only by the metadata, i.e. the date the message was sent, the type of message and the sending and receiving banks involved. The Designated Provider has put in place strong data protection and security measures in order to protect the data of its custumers worldwide. Therefore, in order to enable searches to be run directly on the current Designated Provider server, all these messages would have to be first decrypted. Doing so would be excessive and disproportionate as the Designated Provider server contains more messages than those required for the purpose of combatting terrorism financing. Moreover, a direct access for search purposes would be prohibitively intrusive for the daily operations of the Designated Provider and would create significant operational, security and systemic risks. Therefore, this would require creation of a separate database on EU soil for holding the necessary data of the Designated Provider.

Important investment would be needed to put the system in place and to guarantee its full compliance with the security safeguards. The premises of the Designated Provider or another secure location would have to be adjusted to the specific requirements, IT and technical solutions would have to be developed and maintained, and well qualified staff who would manage and oversee the system would have to be employed and trained.

In this option the EU and the Member States would bear all inconveniences and costs of a mechanism set up only to serve the TFTP, an instrument owned by a third country. At present, this option does not appear to be necessary, proportional, or cost effective as it would not bring additional intelligence benefits, would be be costly and demanding to set up and could create risks to personal data protection.

3.2. An EU equivalent system

A fully centralised EU TFTS was excluded from more detailed assessment due to the lack of a legal base and the small chance that Member States would accept an EU centralised role in what is an area of Member State competence. A fully decentralised system was excluded on the basis that it would have had severe costs implications and a multiplied impact on data protection rights. The three hybrid systems assessed would allow varying degrees of Member State control over the searches that are carried out by them and by the centralised EU body.

Extending the scope of an EU equivalent system to cover Automated Clearance Houses, e-money, and other non-FIN data would provide intelligence benefits by increasing the EU's

ability to track intra-EU payments, and could create a more 'future-proof' system than one dealing only with FIN messaging. However, each addition of a Designated Provider would increase the risk of infringements of data protection rights, and would therefore require a rigid set of conditions, safeguards, and control measures. This would also increase the administrative burden placed on Designated Providers. Adding multiple data providers and messages to create such a complex, organizationally and technically demanding system would also increase costs substantially.

As a consequence of this analysis, any feasible EU TFTS would use only FIN message data, as the Commission believes that the added benefits of using multiple data types and providers do not outweigh the significant cost to private companies and damage to privacy and data protection rights that such a system would entail. Thus, as the EU system would cover only the same Designated Provider and the message type as the TFTP, the quality and quantity of intelligence leads received as well as the data exposure would be comparable to the EU- US TFTP.

As outlined above, there are three options for this EU equivalent system: A) the EU TFTS Coordination and Analytical Service, B) the EU TFTS Extraction Service, and C) the FIU Coordination Service.

Option A would be likely to have a positive impact on the prevention of terrorism and enhancement of security in the EU. Having both EU and Member State teams running searches and analysing results would go some way to ensuring that the specific intelligence requirements of the EU and Member States are fully taken into account and that the system is geared towards the specific "EU threat". However, this improvement is contingent on an increasing willingness and ability of Member States to share information and analysis in the medium to long term. It is unclear to what extent this increased flow of information can be relied upon. Additionally, as Member States would retain the capacity to request searches from the US under the TFTP, this system would need significant Member State buy-in and cooperation if it were to provide a more coherent EU picture.

Option B could have some positive impact on preventing terrorism and enhancing security in the EU. The system would be more responsive to EU threat analyses, as the searches would be run according to the specific intelligence requirements of Member States. However, the

role of the centralised EU body would be limited to conducting searches and transfer of responding data to the requesting Member State; it would act more as a gatekeeper than anything else. As a result of this, there would be no EU-level analysis, and the system would be wholly reliant on Member States sharing analyses with one another, outside the system, if a coherent EU intelligence picture were to be created. The inability of the system to guarantee a uniform approach to definitions of searches would increase the risk of false positives, thereby impinging on data protection and privacy rights.

Option C would be responsive to specific intelligence needs of Member States, and so would have some positive impact on preventing terrorism and enhancing security. However, as national FIUs would be responsible for the searches and analyses of their Member States, this option suffers from the same drawbacks as Option B – a clear picture could only be achieved with the enhanced cooperation of Member States, outside the system. Furthermore, FIUs focus on financial intelligence only, and the divide between this information and the broader intelligence landscape could make it more difficult to see links and spot terrorist financing. There is also a very low level of EU involvement in this option, and capacity would be enhanced primarily at the national level.

All these options would entail significant cost for the EU, Member States and the Designated Provider including, inter alia, the cost of development of IT infrastructure, secure facilities and the cost of tens, if not hundreds, of staff responsible for the management of the system and for the implementation of safeguards and controls. However, each of these possible systems has the potential to contribute to an enhanced European security situation, as they would use threat assessments specific to European needs.

An independent intelligence and investigation tool on European soil would remove the requirement for transfering data to the US. But any EU TFTS would still require extensive data protection safeguards and controls similar to those already in force under the EU-US TFTP Agreement and in any event complying with the EU and Member States' data protection acquis. Any requests for searches on data in EU systems would need to be checked for conformity with the strict purpose limitation to fighting terrorism and its financing, including whether the transfer of data is justified. In particular, qualified independent overseers would be required to verify that each EU and each Member State search was properly authorised and was required for the purpose of fighting against terrorism and its

financing. Secure handling and storage of the data would have to be ensured and unathorized access to the data prevented. An external audit of the proper functioning of the system and all its safeguards would be necessary. All necessary procedures for access to and rectification of personal data and relevant redress procedures would have to be embedded in the system.

In conclusion, in line with the requests from the European Parliament and the Council, the Commission has assessed the possible options for for an EU TFTS, including an extraction and retention regime.

This assessment takes into account the principles enshrined in the Information Management Strategy that was adopted under the Swedish Presidency. Any system set up must be necessary, proportionate, and cost-effective, and must respect fundamental rights. The analysis carried out by the Commission, as detailed above and in the Impact Assessment, shows that each of the feasible options has advantages and disadvantages. The Commission has however disregarded those options that are not feasible, as explained.

In light of the information gathered, the case to present at this stage a proposal for an EU TFTS is not clearly demonstrated.

The Commission welcomes the views of the European Parliament and of the Council on this Communication.