COUNCIL OF THE EUROPEAN UNION

Brussels, 15 July 20011

12957/11

GENVAL 81
JAI 522
ECOFIN 523
DATAPROTECT 75
ENFOPOL 245

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	14 July 2011
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	COM(2011)429 final
Subject:	**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European terrorist finance tracking system: available options**

Delegations will find attached Commission document COM(2011) 429 final.

Encl.: COM(2011) 429 final.

EUROPEAN COMMISSION

Brussels, 13.7.2011
COM(2011) 429 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A European terrorist finance tracking system: available options

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A European terrorist finance tracking system: available options

1. INTRODUCTION

When the Council agreed to 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 the purposes of the Terrorist Finance Tracking Program (EU-US TFTP Agreement)[1], it also invited the Commission to submit to the European Parliament and the Council within one year after the date of entry into force of the Agreement (1 August 2010), "a legal and technical framework for extraction of data on EU territory".[2] The European Parliament has also consistently asked that in the longer term a durable, legally sound European solution to the issue of the extraction of requested data on European soil be envisaged.[3] The Communication "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" also already stated that the Commission will develop a policy for the EU to extract and analyse financial messaging data held on its own territory in 2011.[4] Given the proven effectiveness of the US TFTP, a European system is expected to contribute significantly to efforts to cut off terrorists' access to funding and materials and follow their transactions. Reference can also be made to Article 11 of the EU-US TFTP Agreement, which states that during the course of the Agreement, 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. This Communication is the first stage of the Commission's response to this Article and the Council's invitation. It describes the different steps the Commission has taken to move towards establishing such a "legal and technical framework", and presents the different options under consideration for achieving this goal. It does not at this stage indicate one preferred option – it does however present the relevant points to take into consideration with respect to the options considered. Given the political importance of the issue and its legal and technical complexity, the Commission wishes to inform the Council and the European Parliament of the state of play, and trigger a debate. The Commission considers such further debate useful before presenting, on the basis of an Impact Assessment, concrete proposals.

In this context, it should be stressed that this Communication does not prejudge the proposal that the Commission will put forward. Any future proposal will take into account the discussions mentioned above and the Impact Assessment, which will be based on a study which the Commission has contracted out in the second half of 2010. Given the impact a legislative proposal would have on fundamental rights, and in particular on data protection, the Impact Assessment will pay particular attention to the necessity and proportionality of any measures which the Commission may propose. To that end the Commission will follow the

---

1 OJ L 195, 27.7.2010, p.5

2 Council Decision of 13 July 2010, OJ L 195, 27.7.2010, p.3

3 See for example Resolution P7_TA(2010)0143, and the Explanatory Memorandum to Recommendation A7-0224/2010.

4 COM(2010) 673 final, 22.11.2010. See Action 2 under Objective 2, p. 8.

guidance provided in its Communication on the strategy for the implementation of the Charter of Fundamental rights.[5]

In addition, the Impact Assessment will provide the necessary technical background material, as well as a detailed assessment of all available options. These issues have already been discussed with many stakeholders in this area, including Member States authorities, data protection authorities, Europol and the designated provider. The final results of the study mentioned above will be available only by the end of this year. To support the preparation of an Impact Assessment, the European Commission has organised three expert meetings with the same stakeholders, as well as the U.S. authorities involved in running the TFTP. The options discussed in this Communication build on the preliminary results of the study and the discussions in these expert meetings.

2. GOALS OF ESTABLISHING AN EU TERRORIST FINANCE TRACKING SYSTEM

There are two main reasons for establishing an EU terrorist finance tracking system (TFTS):

- the system must provide an effective contribution to the fight against terrorism and its financing within the European Union;

- the system must contribute to limiting the amount of personal data transferred to third-countries. The system should provide for the processing of the data required to run it on EU territory, subject to EU data protection principles and legislation.

In the United States, the Terrorist Finance Tracking Programme (TFTP) has proven to present significant added value to the fight against terrorism and its financing, benefitting not only U.S. authorities, but also the authorities of the Member States of the European Union and third countries. The recent review of the EU-US TFTP Agreement[6] confirmed that since the establishment of the TFTP in the U.S., more than 2500 reports have been shared with the authorities of third countries, the overwhelming majority of which (1700) have been shared with the European Union. The effectiveness of the U.S. programme and its value for combating terrorism and its financing have also been confirmed in the two reports presented by Judge Bruguière, who was appointed by the European Commission in 2008 to review the programme. The TFTP derived information which was provided to EU authorities included significant leads in relation to a number of high profile (attempted) terrorist attacks, such as the Madrid and London attacks, the 2006 plot to bring down transatlantic flights using liquid explosives, and the 2007 attempted attack on U.S. interests in Germany. The EU Review Team also concluded that it had been provided with "convincing indications of the added value of TFTP to the fight against terrorism and its financing". Given these experiences, there are solid grounds for believing an EU TFTS will also provide significant added value to the efforts of the EU and the Member States to combat terrorism and its financing.

Whilst the effectiveness of the U.S. TFTP for combating terrorism and its financing is not in doubt, serious concerns have been raised in relation with its consequences on the fundamental rights of citizens. These concerns are mainly centred around the fact that the implementation of the EU-US TFTP Agreement entails the provision of large amounts of personal data ("bulk data") to U.S. authorities - the vast majority of this data concern citizens who have nothing to

---

5 COM(2010) 573 final, 19.10.2010.

6 SEC (2011) 438 final, 30.3.2011

do with terrorism or its financing. The data is provided in bulk (on the basis of relevant data categories) rather than on an individual basis (in response to a request concerning one or more individuals), due to the fact that the provider of these data does not have the technical capacity to provide the data on an individualised basis. In addition, in order for the provider to release such data on an individualised basis, it would need to set up a dedicated search and analysis function, which is not required by its business processes, and would entail significant resource implications. Also, requesting data on an individualised basis would mean that the provider would in effect be made aware of which individuals are investigated in the context of terrorism investigations and their financial relationships. This could have an impact on the effectiveness of such investigations.

To compensate for the provision of bulk data, significant safeguards have been put in place to ensure that no misuse of the data can take place, including that the provided data may only be searched and used for combating terrorism and its financing. The recent review of the EU-US TFTP Agreement has confirmed that these safeguards are indeed implemented in accordance with the provisions of the Agreement.

Nevertheless, arguments have been made that the provision to a third State of such large amounts of personal data constitutes an unwarranted infringement of the fundamental rights of these citizens, taking the necessity and proportionality of this infringement into consideration. This is the reason why the Council invited the Commission to present proposals for establishing a "system for the extraction of data to take place on EU territory" – the overall aim is to ensure that the processing of such data would take place in accordance with EU data protection legislation and principles, and in accordance with the EU Charter of Fundamental Rights. In this context, it should be noted that the collection and processing of financial data by public authorities affects the right to the protection of personal data, which is enshrined in Article 16 TFEU and Article 8 of the Charter.

In accordance with Article 52(1) of the Charter, any limitation of these fundamental rights must be provided by law, with the necessary precision and quality to provide foreseeability, and respect the essence of those rights. It must be limited to what is necessary and proportional to meet a legitimate objective recognised by the Union. These principles must therefore be taken into consideration not only when taking the decision whether or not an EU TFTS should be established, but also with respect to the different available options for implementing the system. Therefore, these principles equally affect the choices to be made with respect to such issues as the scope of the system, the applicable retention periods, rights of individuals with respect to access and deletion etc. These issues are not dealt with in detail in the current Communication. They will need to be analysed fully in the Impact Assessment.

Naturally, the possible establishment of a system for extracting the data on EU territory would have consequences for the existing EU-US TFTP Agreement, as recognised in Article 11 (3) of the Agreement which states that since the establishment of an EU system could substantially change the context of this Agreement, the Parties should consult to determine whether the Agreement would need to be adjusted if the European Union decides to establish such a system. All options would therefore also have an impact on the future implementation and consequent re-adjustment of the existing EU-US TFTP Agreement.

3. MAIN FUNCTIONS OF AN EU TERRORIST FINANCE TRACKING SYSTEM

One of the first issues to emerge from the discussions with stakeholders referred to above is that these stakeholders are overwhelmingly of the opinion that if an EU terrorist finance tracking system (EU TFTS) is to be established, it should be established in the interest of providing security to EU citizens. The system should not be set up just to provide relevant information to U.S. authorities – the authorities of the Member States have a real interest in the results of such a system as well. This approach also implies that whilst the U.S. TFTP could certainly provide inspiration as to how such a system could be set up, a European equivalent system would not necessarily have to copy all elements of the U.S. TFTP. Also, an EU system should be set up taking the specificity of the EU legal and administrative framework into consideration, including the respect of applicable fundamental rights as indicated above.

However, any system aimed at tracking terrorist financing in accordance with the main goals outlined above would need to foresee the implementation of the following core functions:

- preparing and issuing (legally valid) requests to the designated provider(s) of financial messaging services for the raw data to be provided to an authorised recipient or recipients. This involves determining the message categories to be requested, how often such messages should be sent, and maintaining contacts with the providers on these issues;

- monitoring and authorising requests to the designated provider(s) for such raw data. This involves verifying whether the request for the raw data have been prepared in accordance with the applicable limitations;

- receiving and storing (processing) the raw data from the designated provider(s), including the implementation of an adequate system of physical and electronic data security;

- running the actual searches on the data provided, in line with the applicable legal framework; on the basis of requests for such searches from authorities of the Member States, the U.S. or other third States on the basis of clearly defined conditions and safeguards, or on the own initiative of the authority (or authorities) entrusted with processing the data;

- monitoring and authorising the running of searches on the data provided;

- analysing the results of the searches, through combining these results with other available information or intelligence;

- distributing the results of the searches (without further analysis) or the results of the analyses to authorised recipients;

- implementing an appropriate data protection regime, including applicable retention times, logging obligations, handling requests for access, correction and deletion, etc.

These core functions would need to be laid down in appropriate legal instruments at the EU level, at the national level, or at both levels, depending on the option chosen.

4. KEY PRINCIPLES WHEN CONSIDERING AVAILABLE OPTIONS

In addition to considerations with respect to the core functions outlined above, the choice between the available options will depend to a large extent on the way in which they deliver on a number of key issues, which are currently considered in the Impact Assessment and discussed further below.

4.1. Effectiveness

The expected effectiveness of the different options in meeting the core goal of combating terrorism and its financing is a key factor. Options which increase possibilities for data sharing and analysis at the international level should be favoured from this perspective, since such data sharing and analysis will increase the effectiveness and provide more added value. In particular, the choice of the organisation(s) which will be entrusted with the analysis of the data, as well as providing the results of the analysis to the appropriate authorities, will have a significant impact on the overall effectiveness of the system, as well as on the amount of data that will be transferred. Even so, in accordance with current practice, Member States should continue to have full control over whether their information or intelligence can be shared with other authorities.

4.2. Data protection

The international sharing and analysis of information and intelligence can only take place within a robust and well developed data protection framework. The effectiveness of such a framework is not only dependent on the applicable legal provisions, enabling data subjects to exercise their rights such as judicial redress, but also on the availability of experienced personnel, such as an independent data protection officer and an independent and experienced data protection control authority. Some of the organisations which could be involved in the possible establishment of an EU TFTS already have such structures in place, whereas for others these would need to be established. Therefore, the data protection implications of each of the different options must be carefully assessed in accordance with the overarching principles concerning the respect of fundamental rights referred to under Part 2 of this Communication.

4.3. Data security

Robust data protection provisions need to be combined with state of the art data security infrastructure and technology. Data security considerations point in the direction of limiting the number of sites where the provided data can be processed, as well as limiting any form of outside access to the data. The most secure solution would be storage at one location with no outside access. Most of the organisations which could be involved in running the TFTS already have secure data processing technologies in place, but not all currently have the capacity to handle data classified beyond the level of EU Restricted.

4.4. Data storage

Data storage could take place either at the national or EU level. At the EU level, storing the data received from the designated provider(s) could take place at Europol or at another EU body, such as the Agency for the operational management of large-scale IT systems in the

area of freedom, security and justice (IT Agency)[7], which is in the process of being set up. Since data storage is inextricably linked to the issues of data protection and data security, the choice for the organisation responsible for storing the data should be closely linked to the data protection and data security regime which these organisations can offer.

4.5. Making use of existing structures and instruments

All options should make use of existing structures as far as possible. This limits costs, and makes it possible to profit from experience gained, as well as from existing infrastructure. Such use of existing instruments demands that the new tasks attributed to an existing organisation fit well with the existing mandate of that organisation. For example, Europol, Eurojust or national judicial authorities may be considered to play the role of verifying and authorising the requests to provide data addressed to the designated provider(s)..

4.6. Cooperation between responsible authorities

The options outlined below offer varying degrees of cooperation and sharing of information and intelligence between national authorities, and between national and European authorities. Different Member States have established different ways in which their national authorities cooperate in combating terrorism, and any action at the European level must respect the limitations established by Article 72 TFEU concerning the prerogatives of Member States with regard to the maintenance of law and order and the safeguarding of internal security. Any EU TFTS must therefore allow for a significant level of control by the Member States of the information and intelligence they are willing to share within the context of such a system. Different approaches to this issue have been developed by a number of the organisations referred to below, some of which could be made directly applicable to the system to be established.

4.7. First general overview of the posible financial impact of the different options

The overall costs of establishing an EU TFTS, and their distribution between the EU and the national level will depend to a large extent on the choice of policy option. Costs will in any case involve:

- costs related to the secure transfer and storage of the data received from the designated provider(s);
- costs related to the development and maintenance of the software necessary for running the searches and providing search results;
- costs related to distributing the search results or analyses to authorised recipients;
- personnel costs for staff running the searches and analysis and distributing the results;
- personnel costs for staff responsible for monitoring and audit functions;
- personnel costs for staff responsible for data protection and citizen's rights.

[7] COM (2010) 93 final, 19.3.2010.

Although detailed cost estimates are not yet available at this stage, initial calculations indicate that the costs of the purely EU approach and all the different hybrid options discussed below would be in the range of 33-47 million Euro initial set-up costs, with an additional 7-11 million Euro required for annual running costs. Different options are described below under Part 6 of this Communication. Option 3 would be the most expensive option, with €43 million set-up costs for the EU and €3,7 for the Member States (combined), and €4,2 million annual running costs for the EU and €6.8 million for the Member States (combined). Option 2 would be the cheapest option, with €33 million setup costs for the EU, and €3,5 million annual running costs at EU level, as well as €3,3 million annual running costs for the Member States (combined). Option 1 would require €40,5 million for EU set up costs, and €4 million annual running costs at the EU level, as well as €5 million for annual running costs for the Member States (combined). Naturally, such costs will be reduced if use can be made of staff of existing organisations, or use can be made of existing infrastructures, as well as soft- and hardware. Costs for setting up and running a purely national system would be significantly higher (390 million set-up costs, 37 million annual running costs), since all Member States would be required to set up highly secure data processing systems and employ personnel to run the system.

These amounts are preliminary and will have to be further analysed and detailed in the light of the outcome of the Impact Assessment.

5. ISSUES TO BE CONSIDERED

Irrespective of the choice between the different options for establishing and running an EU TFTS, a number of relevant questions need to be considered with respect to the scope of a possible EU TFTS. These are discussed below.

5.1. Terrorism and its financing or broader?

Access to financial messaging data is not only useful to combat terrorism and its financing. There is little doubt that such access would also be a valuable tool for combating other forms of serious crime, in particular organised crime and money laundering. However, within the context of the EU-US TFTP Agreement, considerations of proportionality have led to a scrupulously maintained limitation of the use of the data to the purposes of combating terrorism and its financing. The preliminary discussions which have so far taken place indicate that there is a wide-spread consensus that such considerations of proportionality also point in the direction of establishing the same limited scope for a European equivalent system, in line with the general considerations concerning the respect of fundamental rights discussed in Part 2 of this Communication.

5.2. More than one provider?

The EU-US TFTP Agreement is currently limited to requesting data from only one provider of international financial messaging services. Although this provider is clearly the most important world-wide provider of such messaging services, other providers operate on the market as well. Considerations of efficiency and creating a level playing field for all players on the market point in the direction of creating a system which will be applicable to all providers of international financial messaging services. In any case, the administrative burden for companies providing financial messaging services must be taken into consideration in the choice of the available options.

5.3. Only international messaging services or also national?

The EU-US TFTP Agreement is currently limited to requesting data only from providers of international financial messaging services, i.e. messaging services used for effecting transnational transactions, including those between EU Member States but with the exclusion of financial messaging data related to the Single Euro Payments Area (SEPA). An EU TFTS will need to consider also the option of including or not financial messaging services exchanged between Member States or whether it will be limited to international exchange of financial messaging services. Purely national financial messaging services (which are used only in the context of national financial transactions) are currently excluded from the scope of the EU-US TFTP Agreement. Access to such national financial messaging services would be of interest in order to combat terrorism and other forms of crime. However, even leaving aside the question whether access to such purely national transactions should be regulated at European level, preliminary discussions confirmed the view that such access is widely considered to be disproportionate, and should therefore be excluded from the scope of an EU system.

5.4. What type of financial messaging data should be covered?

There are many different types of financial messaging data used in the international banking system. The EU-US TFTP Agreement is currently limited to one particular type of financial messaging data. Access to other types of financial messaging data would be of interest in order to combat terrorism and its financing, and possibly other forms of crime. However, also with respect to this choice, considerations of proportionality and respect of fundamental rights of citizens point towards limiting the scope of the messaging types to be covered by the system. Further details on this technical issue will be included in the Impact Assessment.

6. OPTIONS FOR AN EU TFTS

The options described below are currently being examined by the Commission as part of the ongoing Impact Assessment. They are not necessarily limitative and do not in any case prejudge the final Impact Assessment or choice that would be made by the Commission on its basis.

One of the options which is always considered in the process of preparing new initiatives and their accompanying Impact Assessments is the option to stick to the status quo - which in this case would mean to leave the EU-US TFTP Agreement in place, and not come forward with any proposal for an EU TFTS. This option would not reply to the call from Council and Parliament on the Commission to come forward with a proposal to submit "a legal and technical framework for extraction of data on EU territory" referred to in Part 1 of this Communication. In addition, this option would not contribute to limiting the amount of personal data transferred to third countries and it would not provide for the processing of data on EU territory, subject to EU data protection principles and legislation. The other options discussed in more detail below all present possible ways to establish an EU TFTS.

In theory, all of the core functions of an EU TFTS identified under Part 3 of this Communication could be implemented either at the EU level or at the national level. The functions can also be attributed to one or more different organisations, in line with their existing responsibilities, or new organisations could be created to perform them. Such organisations could either be European or national organisations. This implies that – also in

theory – an exclusively European approach is possible, where all core functions would be attributed to EU level organisations, just as well as an exclusively national approach, where all functions would be performed at the national level. In a general sense, it should also be kept in mind that the choices for a centralised, decentralised or hybrid system in this particular case are not necessarily the same as the choices made with respect to other initiatives involving data processing to combat terrorism and organised crime - each initiative in this area should be judged on its own merits.

Both purely centralised and purely national approaches have significant drawbacks. For example, an exclusively European approach would surely suffer from a disconnect with the law enforcement and intelligence organisations and practices of the Member States, and therefore not be very effective. Without input from the national authorities responsible for dealing with these issues, it would be almost impossible to accurately determine which categories of data would need to be requested from the designated provider(s). The usefulness of the system would also be diminished if queries of the database would take place only on the basis of intelligence available at the EU level - at the current level of EU integration, such intelligence is to a large extent only available at the national level. Also, Member States are unlikely to accept such a purely EU level approach, since it would not offer added value to their own efforts to combat terrorism and its financing. During consultations, the Member states also indicated that this option would be politically hard to accept for legal and operational reasons.

At the other extreme, a purely national approach would run the risk of a diverging implementation in the different Member States, and an increased risk of breaches of data security, due to the need to have 27 different copies of the provided data. A purely national approach would also imply difficulties with respect to the implementation of a harmonised data protection framework, as well as a harmonised approach to (the control of) other necessary restrictions, such as the limitation to terrorism and its financing. Also, with a purely national approach it is unclear which Member State would be responsible for handling requests for searches from third countries, and the added benefit of an analysis of the search results at the European level would be lost. In addition, as indicated above, the costs associated with this option would be significantly higher, since all Member States would be required to set up highly secure data processing systems and employ personnel to run the system.

The preparatory work with stakeholders therefore quickly established that the solutions at the extreme ends of the spectrum of possible options were not supported – a consensus emerged that a hybrid solution, which entails distributing the different functions over different organisations at the EU and the national level, was most likely to offer the best possible results on the two main goals. Although this consensus helps in identifying the most suitable option, the hybrid approach still presents a large number of choices to be made. The sections below describe the three hybrid options which emerged from the current preparatory work as the most plausible ones in a bit more detail – the options are also presented in tabular form in the Annex.

6.1. The EU TFTS coordination and analytical service (option 1)

This option would involve establishing an EU central TFTS unit, with most of the tasks and functions being implemented at the EU level. Issuing requests for "raw" data to the Designated Providers(s), verification of these requests, handling requests for searches and running them, managing search results and forwarding reports to those who requested

searches would all take place at the EU level. However, preparing the requests to Designated Provider(s) could take place in consultation with the responsible authorities of the Member States, and the Member States could also opt to second their own analysts to the central unit to participate in the running of searches. Contrary to the fully centralised option, Member States could request searches to be run on their behalf, similar to the current procedure in place with the US TFTP, or to be run by their own analysts.

Member States would need to share information with the EU central TFTS unit, to 'substantiate' the request and its nexus to terrorism before a search could be initiated, or have their requests "pre-authorised" by national authorities. Such national authorities could be for example national counter-terrorism prosecutors or investigating judges – if they would authorise a particular search on the provided data then the EU central TFTS unit could accept to run such searches without further verification. In that scenario no further intelligence would need to be provided to the EU central TFTS unit. The EU central TFTS unit would forward the results of searches and their analysis, and could also provide information spontaneously. The U.S. and other third countries would also need to request the running of searches, following a similar process.

Monitoring compliance with safeguards and controls would also be centralised, possibly involving oversight by external stakeholders, for example representing the Designated Provider(s) and those appointed as independent overseers. Data protection, integrity and security would also be ensured at the central level.

The key bodies involved in the system could be Europol and Eurojust. The tasks to be executed by Europol and Eurojust must in that case be in line with their missions as established by the Treaty on the Functioning of the European Union (TFEU). Also, it will need to be established to what extent the legal instruments currently regulating their functioning will need to be amended. If Europol were to be chosen as the EU central TFTS authority, it would also deal with requests by data subjects for access, rectification and blocking, all in accordance with its existing legal framework and data protection provisions. The EU central TFTS unit would perform its role in accordance with the existing legal framework, and cases of redress and appeals would equally be dealt with in accordance with existing legal provisions. At national level, national law enforcement authorities would be involved for verifying and authorising requests for searches. The possibility of creating new national bodies could be envisaged, but this choice would best be left to the Member States on the basis of the subsidiarity principle.[8]

6.2. The EU TFTS extraction service (option 2)

As under the first policy option, this one would involve establishing an EU central TFTS unit, whose tasks would comprise issuing requests for "raw" data to the Designated Providers(s), verification of these requests, running searches, and handling requests for searches. However, under this option, the EU TFTS unit would not be allowed to analyse the search results and compare them with other available information or intelligence when such searches are made at the request of the authorities of the Member States – in such cases its role would be limited to preparing and distributing search results in a presentable manner.

---

[8] At this stage, the consequences for the budgets of the EU agencies which might play a role in the implementation of the system are not yet known.

As under the option 1, requests for "raw" data to be issued to the Designated Provider(s) would be prepared in close consultation with the Member States, who could make their specific needs known to the central TFTS unit, which would analyse these and formulate the request(s) based on that analysis.

Member States authorities would request searches to be run on their behalf. The extent to which such requests are substantiated and have a nexus to terrorism would be verified and validated at national level. The EU central TFTS unit would run the search and return the full set of results, organised in a presentable manner, to the Member States. The Member States authorities would be the only ones to undertake the analysis of the searches, and they could also opt for spontaneous provision of information.

The EU central TFTS unit would be charged with conducting searches and analysing the results on behalf of EU institutions, the US and other third countries. It could also spontaneously provide information on that basis.

As under the previous options, monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders, for example representing the Designated Provider(s) and those appointed as independent overseers. Data protection, data integrity and data security would also be ensured at the central level.

Again like under the previous option, the key bodies involved in the system could be Europol and Eurojust. At national level, the key bodies involved would be national law enforcement or intelligence authorities. As before, the creation of new national bodies would be left to the Member States on the basis of the subsidiarity principle. Europol and/or the national units would deal with requests by EU citizens for access, rectification and deletion, involving both national Data Protection Authorities and Europol's Joint Supervisory Body. Cases of redress and appeals would be dealt with in accordance with applicable legal provisions at the national or EU level.[9]

6.3. The Financial Intelligence Unit (FIU) coordination service (option 3)

This policy option would involve the establishment of an upgraded FIU Platform, made up of all the FIUs of the Member States. The ad-hoc EU level authority would issue requests for "raw" data to the Designated Provider(s), by compiling the needs specified by the FIUs into a single request, which would also be verified and authorised at central level.

Each FIU would be responsible for running searches and managing search results on behalf of its Member State, as well as for carrying out analyses and forwarding reports to those it considers relevant. The extent to which searches are substantiated and have a nexus to terrorism would be verified and validated at national or EU level. The FIUs would also be responsible for the spontaneous provision of information.

The upgraded FIU Platform would be able to conduct searches and analyse the results on behalf of EU institutions and other third countries with which the EU will have concluded an agreement. It could also provide information spontaneously.

Monitoring compliance with safeguards and controls would be centralised, possibly involving oversight by external stakeholders, for example representing the Designated Provider(s) and

[9] See footnote 8.

those appointed as independent overseers. Data protection, integrity and security would also be ensured at the central level.

The upgraded FIU Platform would be conferred a formal legal status with clearly defined roles and responsibilities. At national level, the key bodies involved would be the FIUs and national law enforcement and intelligence authorities.

An EU level authority would handle requests by EU citizens for access, rectification and deletion, with cases of redress and appeals dealt with in accordance with applicable legal provisions at the national or EU level.

7. CONCLUSION

On the basis of the preparatory work taken forward by the Commission so far, and subject to the results of the Impact Assessment, this Communication describes the different possible options for the establishment of a "legal and technical framework for extraction of data on EU territory" in the context of a terrorist finance tracking system. The different options identified in this Communication show that important choices and decisions will still need to be made, including as regards the respect of fundamental rights, and many legal, technical, organisational and financial issues will need to be addressed in much more detail in the course of further preparatory work. Given these significant challenges, the Commission considers that sufficient time is needed for further preparatory work and for debate with Council and Parliament.

* * *

Annex: Tabular overview hybrid options

	EU TFTS coordination and analytical service (option 1)	EU TFTS extraction service (option 2)	Financial Intelligence Unit (FIU) coordination service (option 3)
Preparing and issuing requests for "raw data"	EU Central TFTS Unit in coordination with MS	EU Central TFTS Unit in coordination with MS	Upgraded FIU Platform
Monitoring and authorising requests for "raw data"	Eurojust or another existing body	Eurojust or another existing body	Eurojust or another existing body
Receipt and storage of the "raw data", data security	Europol or other EU body such as the IT Agency	Europol or other EU body such as the IT Agency	Europol or other EU body such as the IT Agency
Running searches on the "raw data"	EU Central TFTS Unit, MS seconded analysts or combination of both	EU Central TFTS Unit	FIU's, upgraded FIU Platform
Monitoring and authorising the running of searches	Independent overseers, possibly national authorities	Independent overseers, national authorities	Independent overseers
Analysing the results of the searches	EU Central TFTS Unit, MS seconded analysts or combination of both	National authorities for national searches, EU Central TFTS analysts for EU and third country searches	Upgraded FIU Platform, national FIUs
Distributing the results of the searches	Europol analysts or MS seconded analysts	National authorities for national searches, EU Central TFTS analysts for EU and third country searches	Upgraded FIU Platform, national FIUs
Implementing an appropriate data protection regime	Europol or other EU body such as the IT Agency	Europol or other EU body such as the IT Agency	Europol or other EU body such as the IT Agency