ARTICLE 29 DATA PROTECTION WORKING PARTY

Brussels, 29 September 2011

Commissioner Cecilia Malmström
Commissioner for DG Home B - 1049
Brussels Belgium

Subject: Terrorist Finance Tracking System (TFTS) – European Commission Communication COM (2011) 429

Dear Commissioner Malmström,

As you may be aware the Article 29 Working Party (hereafter the Working Party) has actively contributed to the debate on the coming into force and joint review of the current agreement between the US and EU regarding the Terrorist Finance Tracking Programme (US-TFTP).

The Working Party acknowledges the progress that the European Commission has made to bring forward, in line with the TFTP agreement[1], a Terrorist Finance Tracking System for "the extraction of the requested data on European soil[2]", which is the subject matter of the European Commission's Communication - COM (2011) 429 final of 13 July 2011 (hereafter the Communication) with a view to start discussion and debate on this issue.

The Working Party specifically notes the effort made by the European Commission to identify, as required by Article 2.1 of the Council Decision of 13 July 2010, the modalities for "extraction [of the data] on European soil" and the data to be transferred to the US Treasury, especially the attempt made to remedy the shortcomings of the US-TFTP agreement highlighted by the Working Party and the Europol Joint Supervisory Body amongst others.

The Communication offers only a general overview of the potential main features of the TFTS and highlights a number of changeable elements within the three broad options described. The Working Party notes that it is unclear as to the Commission's intention with regard to the EU-TFTS and therefore it is important, to highlight that, whether the Commission intends to remain with the status quo, remedy the shortcomings of the current US-TFTP or whether it intends to create an entirely new EU-TFTS, the outcome of each may require a different legal basis and therefore its impact on the proportionality and necessity of the proposed system should be assessed. Given this uncertainty, the Working Party is unable, at this stage, to provide a full assessment of the data protection issues until the TFTS has been sufficiently defined, ie in terms of its legal basis, architecture and functions. These issues will be complemented by a comprehensive analysis of data protection issues based on the development of the TFTS project, the findings of which the Working Party will report back to the Commission when completed. However it must be stressed that the overarching point here is that, at present, the Working Party has no evidence that the processing of personal data for such purposes is necessary, proportionate and legitimate to the present problem.

1 Articles 2 and 3 of the Council Decision of 13 July 2010(2010/4512/EU, O.J., 27 July 2010)
2 Resolution P7 TA (2010) 0143 of the European Parliament

The Working Party does note, however, some positive elements of the Communication, particularly the call for a robust and well developed data protection framework, which will ensure the processing of financial data for the fight against terrorism is in compliance with European data protection principles and legislation. The Working Party agrees with the suggestion that any potential TFTS must be targeted in a way that corresponds with EU needs; that it should not be a copy of the US TFTP; and that Member States should continue to have full control over their information and intelligence with other authorities (particularly when this relates to third countries). The Working Party also supports the call that state of the art security would be required to ensure compliance with the data protection security principle.

Whilst the Communication does indeed offer some important and positive elements, the Working Party offers the Commission some initial and overarching points which it should consider before refining its proposal for the TFTS further.

Necessity and proportionality

The Communication rightly refers to Article 16 of the TFEU and Article 8 of the Charter of Fundamental Rights of the European Union, establishing the fundamental right to the protection of personal data. The Communication also refers to Article 52(1) of the Charter of Fundamental Rights which states that any limitation on these [fundamental] rights needs to be, a) provided by law and b) with the necessary precision and quality to provide forseeability, and respect the essence of these rights. Reference could also be made in this regard, to Article 8 of the European Convention on Human Rights, as interpreted in case law of the European Court of Human Rights.

Given the above laws referred to, it must be re-iterated whether it is the intention of the Commission to create an entirely new system in the EU for the tracking of terrorist financing or simply amend the shortcomings of the current US-TFTP agreement – the Working Party remains unconvinced that either possibility meets the test of necessity and proportionality. Whilst the TFTS would go some way to addressing to remedying the shortcomings of the EU-US Agreement, the Working Party would like to make it clear that it is calling upon the Commission to ensure that its Impact Assessment includes convincing and unequivocal evidence as to the **necessity** of the TFTS for the purposes of counter terrorism. The fact that such a system would just provide 'added value' to the international counter-terrorism effort, however true and important that may be, it does not demonstrate necessity or the precision needed to be considered as a "purpose" for processing.

There is a lack of clarity in the scope of the system which could lead to controllers of financial data making suspicious transaction reports on a large part of the global population rather than limiting the reports to those for whom there is suspicion – leaving the potential for the development of a system which is disproportionate to its intended purpose. Furthermore although the objective to limit the transfer of bulk data to the US is to be supported, this cannot be the basis for the development of a similar system within the EU – as again this does not meet the test of necessity and proportionality.

The Working Party is concerned that, if progressed, the Commission's proposal would commit it to the establishment of a highly intrusive and large scale data collection system that will infringe on the fundamental rights of many individuals. Therefore to address the concerns outlined above, the Working Party believes the TFTS should be:

- demonstrably necessary to address the problem – particularly if it is the Commission's intention to create an entirely new EU-TFTS (ie taking into account the existing harmonised EU legal frameworks - the fight against anti-money laundering

and terrorism financing legislation and the on-going activities in the field run by Europol and other forms of police and judicial cooperation (eg collection of evidence and the rights of the suspect));

- demonstrably likely to address the problem;
- proportionate to the security benefit;
- demonstrably less invasive than alternative measures; and
- regularly reviewed to ensure that the measures are still proportionate.

It may be premature to discuss the three broad options outlined in the Communication before the case as to the legality and necessity of the TFTS has been made, but the Working Party considers it helpful to highlight some of the potential issues with these options, as outlined, to the Commission. However, the Working Party witholds its full assessment of this issue until a more refined option/set of options has been developed.

- Option 1
  It is understood that in this scenario, Europol, Eurojust and even national competent authorities could be the validating and authorising authorities for the requests. The Working Party notes that the European Parliament amongst others has already expressed concerns that Europol was the designated judicial authority to carry out oversight of the US-TFTP. In his Opinion of June 2010, the European Data Protection Supervisor made his views clear stating that: *"It is obvious that Europol is not a judicial authority"*. Concerns were also raised about the independence of Europol, given that, if it were to administer such a system, Europol itself would perhaps indirectly benefit from the US-TFTP with potential leads given to it from its US counterparts as a result of information from SWIFT.

  Furthermore, the Working Party would also like to highlight the issues already raised by the Europol Joint Supervisory Body in its report of March 2011 on the US-TFTP Inspection carried out in November 2010 which concluded that some data protection requirements were not being met – particularly that approved requests, when written, were too broad and abstract and not specific enough, and in some cases, given orally, and therefore not in line with the agreement.

  It is clear from the above that, if Europol were to be confirmed as part of the TFTS framework, its role must:

  - strictly adhere to its existing legal framework and data protection provisions;
  - not form part of the judicial oversight of the system (similar concerns exist for Eurojust);
  - be improved given the issues highlighted by the Europol JSB and its recent review of the US-TFTP, ie make robust improvements to verification processes by ensuring that requests are specific, narrowly tailored and written; and
  - avoid duplicating the US-TFTP literally and therefore avoid a repeat of the issues with the current US-TFTP agreement highlighted in this letter and other contexts.

- Option 2
  Option 2 presents the case for Member States' judiciary to authorise requests for raw data by competent national authorities. Whilst not an immediate data protection issue, the Working Party would like to ensure that, at the very least, authorisations are consistent across all Member States.

With regard to data protection and option 2 more specifically, it is unclear from the Communication what the raw data will consist of. Although Europol's role in this option is to search the data, it is unclear to the Working Party as to what the raw data will provide and whether this is in compliance with the data minimisation principle.

- Option 3
  Option 3 provides a new legal status to be conferred on a new Financial Intelligence Unit (FIU) platform. FIUs are (pursuant to, amongst others, Directive 2005/60) the competent authorities responsible for anti money laundering and counter terrorism finance initiatives, The Working Party urges the Commission, if this options is taken forward, to make sure that the legislative proposal is clear on what powers the FIU platform would have, again perhaps noting the issues already raised about the independence and nature of Europol in the US-TFTP agreement. The Working Party is also concerned to ensure that sufficient oversight of this body is required from the National Data Protection Authorities (NDPA). As has been the case with the current US-TFTP, concerns regarding sufficient NDPA involvement and judicial redress have been expressed by the Working Party (as well as the European Parliament), and we therefore urge the Commission to ensure that such issues are not repeated with the TFTS and are addressed.

Data controller and processor relationships
There is no firm decision regarding which authority will have data controllership or processing responsibilities as yet, because this depends on the final set up of the TFTS. Whichever mix of authorities is proposed, the Commission will need to carefully consider and define who controls the data and what they will be doing with it.

Bulk data transfers
It is important to note that the Working Party has already, and continues to express, its concerns that the request for, and transfer of, bulk data is not proportionate or in line with the data minimisation principle[3].

Concerns regarding bulk transfers of this data have already been highlighted in the context of the current US-TFTP. The Communication states "*the system must contribute to limiting the amount of personal data transferred to third countries. The systems should provide for the processing of the data required to run on it on EU territory, subject to EU data protection principle and legislation*[4]*.*"

[3] Article 29 Working Party Opinion WP186 – Processing personal data for anti money laundering and counter financing terrorism purposes. Recommendations 37-41

[4] Communication from the Commission to the European Parliament and the Council, A European terrorist finance tracking system: available options, Page 2, Section 2

However, it is also clear from the Communication that this issue may not be fully resolved with the creation of the TFTS, nor would its aim of limiting the data to be transferred be met. Technical problems have been pointed to in the past for not being able to overcome this point, and the Communication cites the issue of individualised searches meaning that the provider becomes aware of those being investigated and this may result in infringing or impeding the investigation. Neither of these arguments is valid from a data protection point of view. Data processed must be "adequate, relevant and not excessive" and it must have a purpose. Any data being processed which does not fall within the purpose of the processing will clearly be inadequate, irrelevant and excessive. Therefore bulk data will not meet this principle. The Communication also makes reference to "raw data". It is possible, given that it is not defined in the Communication this may not be in compliance with the data minimisation principle either and could also be classed as a "bulk transfer".

Given the stated aim of sending less data to third countries, the Commission should also consider both the impact that any new TFTS would have on the current US-TFTP agreement, and take steps to ensure that the most appropriate technical and organisational measures be put in place to meet the test of necessity and the principles of proportionality and limitation. The Working Party would find it difficult to accept any justification which allows the continuation of the US-TFTP agreement in parallel with the establishment of the TFTS.

Therefore, the Working Party's view is that the Commission should:

- carefully define the data that is being processed;
- ensure the data being processed and/or shared meets the necessity test;
- make sure all competent authorities focus on ensuring sufficient safeguards, such as that of confidentiality rules are in place for all personnel handling such information, rather than allowing any transfers of bulk data; and
- reassess the necessity and proportionality of the current US-TFTP if the EU-TFTS is implemented and amend/terminate as appropriate.

Type of data being processed and shared

The Communication opens a debate as to whether international and national messaging services as well as the specific types of messaging data should be included in TFTS or not. These elements should link back to the issues highlighted above, about purpose, proportionality and necessity, and the principles of limitation and minimisation. Clearly until the Commission has developed these ideas further, the Working Party cannot give any comprehensive assessment. However once these elements have been developed, the Working Party will of course provide further comments.

Retention

Directive 95/46/EC sets a clear goal for any data controller to ensure that: "Data must be: Adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed".

Therefore it is important that any option proposed makes a clear and justifiable case for any retention mechanism either by the Member State's competent authority, the EU central TFTS unit or any other parties involved. The Working Party has expressed its concerns on many occasions (ie US-TFTP and PNR agreements amongst others) that blanket retention periods should not be imposed and that retention mechanisms should be based on need.

Different retention mechanisms could be envisaged depending on the nature of the data itself, how it is being processed and who is doing the processing. For example, retention mechanisms stored will need to take account of how and where the data is being stored eg the timescales involved for retaining, archiving or deleting the data; if it is stored in a single location or on multiple sites (and indeed if those sites are in one or more jurisdictions); and the technical and organisational measures to meet the security principle.

Consideration must also be given to access controls, for example how, who, when and why the data is being accessed will all be some of the defining factors in creating the most appropriate retention mechanism suitable for the specific parties involved. Whatever the context, there is little doubt that the data should be defined under specific, clear and strict definitions and that special attention and safeguards should be provided to sensitive personal data. Any retention mechanism developed must be necessary and proportionate to the nature of the data in question.

Rights of data subjects, judicial redress and oversight

The Working Party welcomes the fact that the Communication acknowledges the need for the development of more legal certainty with regard to data subjects being able to enforce their rights and obtain judicial redress. To attain this, the Working Party urges the Commission to ensure that legal certainty is brought to EU citizens through the existing provisions within the data protection legal framework rather than creating any specific or new arrangements through the TFTS.

The Working Party has already addressed the issue of rights of access pursuant to the current US-TFTP agreement in its letter of 7 June 2011 addressed to the US Treasury, copied to the Commission and is awaiting a reply.

In this regard, the Working Party recalls the examples raised in the context of the joint review of the EU-US TFTP Agreement. It was noted on that occasion that only access requests regarding the so-called *extracted* data were considered by the US Treasury. Furthermore, given the security exception, it was considered unlikely that citizens could actually receive confirmation of the processing of their information within the framework of the US-TFTP. Any European system should learn from this and allow for searches against the full database, based upon the explicit and informed consent of the requestor, in order to fulfil any access request.

The Working Party also seeks assurance from the Commission that the rights of access for individuals and an active oversight role for National Data Protection Authorities (NDPAs) will be carefully considered, clearly outlined and respected by all parties. This would help overcome the current issue that some data subjects are being denied their rights such as access and redress under the current US-TFTP agreement. A potential solution to the specific issue of subject access, for example, could be for any new arrangement to ensure that NDPAs are permitted access to all information relating to the complaint in order to make an informed decision – similar to that of the Europol Appeals Committee.

Competence, independence and coordination

The Working Party also notes that little information is given about the precise roles of any active oversight mechanisms including the role of NDPAs. Until the relationships of all component authorities are developed further, the implications of any oversight mechanism are difficult to assess, however the Working Party would expect that due consideration and respect is given to the role and competencies of NDPAs, independently of and jointly with EDPS and joint supervisory bodies, particularly in: - coordinating supervision and avoiding

contradictions, gaps or conflicting competencies. Any proposal should be fully compliant with the data protection legislative framework in the EU, as defined in Directive 95/46/EC, Framework Decision 2008/977/JHA and the Europol Decision. The Working Party is hopeful that the Commission shares its view that a single, clear and well defined oversight mechanism is envisaged where NDPAs can play an active and independent role. Furthermore, the proposal should take into account the changes to the data protection legislative framework that the Commission is currently preparing. The Working Party urges the Commission not to create yet another custom data protection arrangement, as this is neither in the interest of the individuals concerned nor of the parties involved.

Data security and storage

Data security is another issue that needs to be fully considered as part of the data protection requirements. In particular, the security measures should reflect the need to adequately protect the data and systems in light of the risk posed by the processing operations during the entire data life cycle. This includes specific rules on the accountability and responsibility of data controllers and processors. One example is that the Communication mentions storage in one location with no outside access as the "most secure solution". This would be the most effective and secure way only if the data was processed at this facility, if no copies or downloading were allowed and the data was deleted once it was sent on to the Member State. However the Communication does not make clear if this would be the case.

Co-operation

Finally, it is important that the Commission has already recognised that there is significant divergence in Member States' approaches to information sharing. However, any existing or future cooperation procedures must fit with the appropriate binding legal frameworks. For example by ensuring transparency; making sure there are appropriate guarantees and safeguards for onward transfers; and ensuring suitable redress mechanisms are established.

Conclusion

The above outline cannot be seen as a substantive assessment of the data protection implications of the EU-TFTS programme. The Working Party will continue to monitor the development of the EU-TFTS and contribute further to the debate set in motion and present further analyses of the proposed system as is necessary. However, the Working Party trusts that its considerations and advice will contribute to the Commission's effort to put forward a legislative proposal and remains at your disposal for further consultation.

Yours sincerely

Jacob Kohnstamm Chairman

c.c. Council, European Parliament
V. Reading, Commissioner for Justice, Fundamental Rights and Citizenship