COUNCIL OF THE EUROPEAN UNION

Brussels, 24 April 2014 (OR. en)

9164/14

**JAI 254
DATAPROTECT 62
ECOFIN 413
GENVAL 25
ENFOPOL 118**

NOTE

From:	European Data Protection Supervisor
To:	Delegations
No. Cion doc.:	17063/13 JAI 1092 DATAPROTECT 187 ECOFIN 1091 GENVAL 85 ENFOPOL 398
Subject:	EDPS comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working Document - Impact Assessment accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS)

Delegations will find in Annex European Data Protection Supervisor's comments on the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) and on the Commission Staff Working Document - Impact Assessment accompanying the Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS).

ANNEX

I. Introduction

a) Context of the Communication

1. The EU-US Terrorist Finance Tracking Program (TFTP) Agreement[1], in force since 1 August 2010, sets out the legal framework for the transfer of financial payment messages stored in the EU to the US Treasury Department (UST) for the purposes of preventing, investigating, detecting and prosecuting terrorism and terrorist financing. The agreement also provides for the sharing of relevant information obtained by the UST through the TFTP with competent authorities of the EU Member States, Europol and Eurojust for the same purposes[2].

2. As requested by the Council and the European Parliament[3], the Council decision on the conclusion of the EU-US TFTP Agreement invited the Commission to submit a legal and technical framework for extraction of data on EU territory within one year of the date of entry into force of the Agreement, and to present a progress report on the development of an equivalent EU system within three years of the date of entry into force of the Agreement. The Agreement also requires the Commission to carry out a study of the possible introduction of an EU system equivalent to the TFTP "allowing for a more targeted transfer of data"[4] from the EU to the US.

---

1 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, OJ L 195, 27.7.2010.

2 Article 1 paragraphs (a-b) of the EU-US TFTP Agreement.

3 See Article 2 of the Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010 and the Recommendation of the European Parliament on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, A7-9999/2010, 5.7.2010.

4 Article 11 of the EU-US TFTP Agreement.

3. The study was contracted by the Commission in December 2010 and extended in July 2011 to cover the possibility of an EU retention and extraction regime[5]. After issuing a Communication in 2011, the Commission presented the possible options in October 2011 in the JHA Council and in the Civil Liberties Committee of the European Parliament.[6] Since the Member States and the European Parliament did not express a clear preference for any of the options, the Commission decided to look at all of them[7] in an impact assessment, which has been the basis for a new Communication.

b) Consultation of the EDPS

4. The Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS)[8] (hereinafter: "the Communication") was adopted on 27 November 2013. It was accompanied by the Commission Staff Working Document - Impact Assessment on European Terrorist Financing Tracking System (TFTS)[9] (hereinafter: "the Impact Assessment").

5. The EDPS had been previously consulted and used the opportunity to provide informal comments. The present comments aim at making our views publicly available.

5 See Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTS) (COM(2013) 842 final), p.3.
6 *Idem.*
7 *Idem.*
8 COM(2013) 842 final.
9 SWD(2013) 488 final.

II. General comments

a) The scope of the analysis of the impact on fundamental rights

6. The EDPS welcomes the analysis "of the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness"[10]. This analysis has been applied to the assessment of the policy options implying the creation of an EU TFTS or an EU framework for extraction of data on EU territory. In light of these principles, the Communication concludes that "the case to present at this stage a proposal for an EU TFTS is not clearly demonstrated".

7. The EDPS welcomes this conclusion and the reasoning leading to it. However, he regrets that the analysis of the principles mentioned above has not been sufficiently taken into consideration as regards the options involving the continuation, amendment or termination of the EU-US TFTP Agreement[11]. Such assessment is even more relevant in light of the judgment of the Court of Justice of 8 April 2014 on the data retention directive (Joined cases C-293/12 and C-594/12).

8. In addition, the EDPS regrets that the impact assessment[12] does not include a detailed analysis of options that due to a possible lack of political support, among other reasons, have been *a priori* discarded. In order to allow for a sufficiently informed decision-making, these options should have also been analysed (see further section III sub a below).

9. The request by the European Parliament and the Council of a study on a possible EU TFTS is directly related to the negotiation of the TFTP Agreement and to its expected impact on the rights to privacy and data protection of EU citizens. Therefore, any analysis of such impact as regards a similar system in the EU should also fully take into consideration the impact of the EU-US TFTP Agreement.

[10] See p. 4 of the Communication.
[11] OJ L 195, 27.7.2010, p. 3.
[12] See p.23-26 of the Impact Assessment.

b) The relevance of the reports of the Joint Supervisory Body of Europol

10. The EDPS also regrets that the assessment of the options relating to the EU-US TFTP Agreement does not take into consideration the conclusions of the reports of the Joint Supervisory Body (JSB) of Europol on the inspections of the implementation of that Agreement.

11. The public version[13] of the last JSB reports confirms that under the EU-US TFTP Agreement, the US submits an average of one request per month, each covering a period of one month, and all having a similar geographical scope. The JSB concludes that if it is not possible to narrow the time frame or the geographical scope of the requests, this could indicate that it is not possible to fulfil all intended safeguards of Article 4 of the Agreement (see also section III sub c2 below). These considerations should have been integrated in the Communication and the Impact Assessment and analysed in light of "the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness" mentioned by the Communication.

III. Specific comments

a) Discarded options A.2 and A.3

12. The detailed analysis of impacts is limited to the "short listed options". This excludes the option called "status quo plus" (A.2), i.e., amending the EU-US TFTP Agreement and the "zero option" (A.3), i.e., terminating the current EU-US TFTP Agreement.

13. Option A.2 would provide for amendments to the Agreement in order to ensure a higher EU involvement in the TFTP. Some of the reasons to discard this option are the dependence on a third country's consent and the possible lack of political support at national and EU level. However, political support at EU level[14] and the willingness of a third country to provide consent may vary. Excluding this option *a priori* from the assessment may prevent legislators and policy makers from taking future political decisions on appropriately informed bases. This is also valid as regards option A.3, involving the termination of the EU-US TFTP Agreement.

13 The JSB final reports are classified as EU SECRET. The public versions are available on http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

14 See for example the European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance.

14. The argument that option A.2 would not guarantee a positive impact on data protection and that it would imply high implementation costs is also questionable, as it will depend on how the Agreement is amended. Several sub-options should have been added and assessed in this regard, contemplating different possibilities to amend the EU-US TFTP Agreement.

15. As regards option A.3, the Impact Assessment states that the fact that intra-European zone data would be excluded would make the system "even less adapted to EU intelligence" needs and would thus "considerably worsen the current situation". This statement should be carefully evaluated taking also into consideration the impact of the EU-US TFTP Agreement (and the potential impact of its termination) on the fundamental rights to privacy and data protection, as well as its necessity and proportionality as regards the prevention of terrorist offences in the EU.

b) Options B

16. Options B relate to an EU TFTS or an extraction framework on EU territory. They include a centralised system at EU level (B.1), a decentralised system at Member states level (B.2) and hybrid systems (B.3).

b1) Impact on fundamental rights, necessity and proportionality

17. As stated above, the EDPS supports the analysis provided in point 2.1 of the Communication of "the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness" as regards the TFTS. The same analysis should be applied to the assessment of options A (see sub a above and sub c below).

18. Point 3.1 of the Communication states that "the extraction of the data on European soil instead of in the US would not guarantee better protection of personal data per se"[15]. This general statement should be nuanced. Under the same conditions of protection, the sole fact that the system is established in the EU would for example allow for direct supervision by EU Data Protection Authorities or the EDPS and ease access to appropriate administrative and judicial redress. Moreover, in its judgment on the data retention directive mentioned above in point 7 the CJEU stresses the fact that where there is no possibility of effective control by an independent authority - and therefore, no possibility to check compliance with the requirements of protection and security - personal data should not be retained regardless of the territory, be it Europe or elsewhere. Also for this reason, the establishment of an equivalent system to the TFTS system on European grounds should be considered as an important factor in the assessment of the necessity and the proportionality of the measure.

b2) Scope of the requests

19. The Communication also states that "under the EU-US TFTP Agreement the US does not have access to all data of the Designated Provider but only to the sets of data it requested and approved by Europol on the basis of past and current terrorism risk analyses"[16]. It further states that "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". [17]

20. However, it is questionable whether requests conducted under the EU-US TFTP Agreement are actually "initially narrowed" (see below) in view of the technical limitations and security restrictions acknowledged by the Communication as regards the Designated Provider.[18]

---

15 See p. 9.
16 See p.10. This text should probably read: "... and that were approved by Europol”.
17 *Idem.*
18 *Idem.*

c) Option A.1 keeping the status quo: the continuation of the TFTP

c1) Necessity and proportionality

21. The Impact Assessment states that the EU-US TFTP Agreement, "as confirmed by the two reviews", is "a valuable instrument" for EU-US cooperation in the fight against terrorism and that "it also has turned out to increasingly serve EU security needs by enhancing reciprocity"[19].

22. However, as stated in the Communication[20], limitations on the exercise of the rights and freedoms recognised by the EU Charter of Fundamental Rights are only allowed if, subject to the principle of proportionality, 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. Therefore, the Impact Assessment should not only assess whether the Agreement is valuable but also whether it is necessary and proportionate. This analysis should clearly focus on EU security needs, rather than on US ones.

23. In addition, account should be taken of the recent revelations on large-scale US intelligence collection programmes, which include allegations that the PNR agreement and the TFTP agreement may have been breached[21]. While, according to the Commission, there is no evidence of such breach, the EDPS is not aware of any investigation being conducted specifically in relation with the allegations.[22]

c2) Scope of the requests

24. The Communication states that "Europol verifies that the requests for data received from the US are in conformity with the Agreement and, in particular, that they are as narrowly tailored as possible in order to minimize the volume of data that is transferred"[23].

---

[19] See p. 25.
[20] See p. 4.
[21] See the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows".
[22] The above mentioned Communication states that neither the joint review of the implementation of the PNR Agreement nor the formal consultations opened by the Commission on the TFTP Agreement "revealed any elements proving a breach of these agreements", and that the US have provided written assurance that no direct data collection has taken place contrary to the provisions of the TFTP Agreement.
[23] See p. 7.

25. Article 4 of the EU-US TFTP Agreement provides that the US Treasury Department can request data from designated providers[24] and that it has to simultaneously provide a copy of the request to Europol[25]. After Europol receives the copy of the request it shall urgently verify whether the request complies with the requirements of Article 4(2)[26]. This includes checking whether the request clearly substantiated the necessity of the data[27] and if the request was tailored as narrowly as possible in order to minimise the amount of data requested[28].

26. However, the Communication puts into question the technical feasibility of narrow requests in its analysis of a possible EU TFTS or EU extraction framework[29]. This issue has also been raised by Europol's Joint Supervisory Body (JSB) in its second and third inspections of the implementation of the TFTP Agreement[30].

27. Even if it did not have access to information on the amount of data transferred, the JSB found that Europol receives on average one request per month, each of them covering a period of one month and having a similar geographical scope. The JSB concluded in its second report that if narrowing the requests' time frame or excluding data relating to certain countries/territories is actually "impracticable due to the nature of the programme", it might be impossible to fulfil Article 4 of the Agreement. In its third inspection report, the JSB reiterates that "in view of the nature of the TFTP and the scope of the agreement there is massive, regular data transfer from the EU to the US".

28. In this regard, the EDPS notes that "the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness" should not only apply to the further processing of the data by US authorities, but also to its initial collection or transfer from the Designated Providers.

---

[24] For the list of designated providers see the Annex of the TFTP Agreement. Currently the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the only designated provider and as Article 3 of the TFTP Agreement provides, any amendments to the Annex will be published in the Official Journal of the European Union.

[25] See Article 4(3) of the TFTP Agreement.

[26] Article 4(4) of the TFTP Agreement.

[27] Article 4(2) (b) of the TFTP Agreement.

[28] Article 4(2) (c) of the TFTP Agreement.

[29] *Idem.*

[30] Public versions of the reports are available on http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

29. Therefore, the EDPS questions the conclusion in point 3.1 of the Communication that a framework for extraction of data on EU territory would increase the (negative) impact on data protection rights with respect to the status quo option unless a mechanism of initial narrowing similar to the one provided by the TFTP Agreement is put in place.

c3) Verification of the requests

30. As mentioned above, the Communication states that the Agreement "regulates thoroughly the process of requesting the data by the US authorities. Europol verifies that the requests for data received from the US are in conformity with the Agreement and, in particular, that they are as narrowly tailored as possible in order to minimize the volume of data that is transferred."

31. As previously stated by the EDPS and the Article 29 Working Party, verification by Europol should not be considered as a sufficient safeguard, as this task should be carried out by a judicial authority. The independence of verifications could be introduced in options B and could also be considered in relation with option A.2, as advised by the 2010 Commission proposal for a mandate[31] and as requested by the European Parliament.

c4) Access to effective judicial and administrative redress

32. The Communication states that "the Agreement provides for persons, regardless of nationality or country of residence, to have available under US law a process for seeking judicial redress from an adverse administrative action".[32]

33. However, the Article 29 Working Party has noted that access and redress are limited to so-called "extracted" data, which might exclude data requested by the US but not further subject to individual searches. It has also noted that the security exception makes it unlikely that data subjects could actually receive confirmation of the processing of their data under the Agreement[33].

---

[31] EU-US data protection agreement negotiations: frequently asked questions European Commission - MEMO/10/216 26/05/2010.

[32] See p. 9.

[33] See Article 29 Working Party letters of 7 June 2011 to the US Treasury and of 29 September 2011 to Commissioner Malmström.

34. The EDPS would recommend completing the Impact Assessment by taking into consideration these elements in the analysis of option A.1, of options B when compared with options A, and in the decision of discarding options A.2 and A.3.

IV. CONCLUSIONS

35. The EDPS welcomes the efforts that were put into analysing the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness of the policy decisions regarding the possible creation of an EU TFTS system or an EU framework for extraction of data on EU territory. However, such principles should also be taken into consideration in the analysis of the impact of the possible continuation, amendment or termination of the EU-US TFTP Agreement on data protection rights.

36. In particular, the EDPS recommends the following:

- fully analysing the impact on the fundamental rights to privacy and data protection of the policy options and sub-options regarding the possible continuation, amendment or termination of the EU-US TFTP Agreement;
- taking into consideration the conclusions of the reports of the Joint Supervisory Body of Europol on the inspections of the implementation of the TFTP Agreement;
- assessing not only whether the EU-US TFTP Agreement is valuable but also whether it is necessary and proportionate; and focusing the analysis on EU security needs;
- conducting an appropriate investigation in order to address the allegations that the PNR agreement and/or the EU-US TFTP agreement may have been breached;
- applying the principles of safeguarding fundamental rights, necessity, proportionality and cost-effectiveness not only to the further processing of the data by US authorities, but also to their initial collection and transfer from the Designated Providers;
- not considering the verification by Europol as a sufficient safeguard, as this task should be carried out by a judicial authority;
- including in the analysis the considerations of the Article 29 Working Party as regards limits to effective judicial and administrative redress under the EU-US TFTP Agreement.

Brussels, 17 April 2014