Opinion of the European Data Protection Supervisor

Proposal for a 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 purposes of the Terrorist Finance Tracking Program (TFTP II)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2],

HAS ADOPTED THE FOLLOWING OPINION

I. Introduction

1. On 15 June 2010, the Commission adopted a Proposal for a 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 purposes of the Terrorist Finance Tracking Program (TFTP) (hereinafter "the proposal"). The proposal (including the text of a draft agreement with the United States) was sent to the EDPS for consultation. The EDPS welcomes this consultation and recommends that a reference to this opinion is included in the preamble of the Proposal.

2. The Commission proposal is triggered by the changes in the architecture of SWIFT[3], which as from 1 January 2010 ensures that SWIFT financial transaction

1 OJ 1995, L 281/31.

2 OJ 2001, L 8/1.

3 SWIFT is a Belgian-based company globally providing messaging services to financial institutions. Since 2001, the US Treasury has served administrative subpoenas on SWIFT in order to access some of the personal data relating to financial transactions,

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

messages which are internal to the European Economic Area and Switzerland will remain within the European zone - as different from the transatlantic zone - and will no longer be mirrored in the US operating centre.

3. With the current proposal the Commission envisages an international agreement between the EU and the US, which, based on Articles 216 (international agreements), 82 (judicial cooperation) and 87 (police cooperation) of the Treaty on the Functioning of the European Union, would require transfer to the United States Department of Treasury of relevant financial messaging data which are necessary for the purpose of the U.S. Treasury Department's Terrorist Finance Tracking Programme.

4. In particular, further to the decision of the European Parliament of 11 February 2010 to withhold its consent with regard to the interim agreement signed on 30 November 2009, the new draft aims at addressing in particular the concerns with regard to the protection of personal data, a fundamental right which after the entry into force of the Lisbon Treaty has acquired even more relevance in the legal framework of the European Union.

5. The proposal highlights the relevance of data protection by explicitly referring to relevant articles of the Treaties and of other international instruments and by acknowledging its nature of fundamental right. However, it does not envisage using Article 16 TFEU as a legal basis, despite the fact that Article 1.1 of the proposed agreement underlines a high level of data protection as one of its main purposes. In this regard, the EDPS reiterates that this agreement not only relates to the exchange of personal data, but also to the protection of these data. Article 16 TFEU is therefore not less relevant as legal basis than Articles 82 and 87 TFEU relating to law enforcement cooperation that have been chosen as legal bases.

6. The proposal is subject to the procedure of Article 218 (6) TFEU. According to this procedure, the Council can only adopt a decision authorising the conclusion of the agreement after obtaining the consent of the European Parliament. This proposal thus represents a crucial "test-case" in applying the new Lisbon procedures to an international agreement on the protection of personal data. Ensuring that data protection principles and safeguards are satisfactorily laid down in this agreement will pave the way to be successful in other negotiations.

7. In this context, the EDPS underlines the importance of the negotiations for an agreement between the European Union and the United States of America on protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters. The draft mandate to start these negotiations was adopted by the Commission on 26 May 2010. In the presentation of this draft mandate, the Commission emphasised the need for a solid agreement on personal data protection.[4]

---

mirrored on a server located on US territory.

4 See Press Release, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/609&format=HTML&aged=0&language=EN&guiLanguage=en

8. Against this background, the EDPS recommends adding to the current proposal a strong link to the negotiations with the US on this general transatlantic data protection framework. It should be ensured that these standards would be applicable also to the TFTP II agreement. The EDPS recommends including this requirement in the current agreement, or at least agreeing with the government of the United States that a possible future agreement on data protection would cover the exchanges foreseen under the present proposal.

9. Finally, the EDPS is actively contributing to the positions of the Article 29 Data Protection Working Party and of the Working Party on Police and Justice. Besides the points made or to be made in those positions, this opinion analyses the current proposal by building on earlier comments of the EDPS, relating to both the interim agreement and the ongoing negotiations with the United States.

II. Analysis of the proposal

II.1 The proposal contains some improvements

10. The EDPS acknowledges that this proposal envisages certain substantial improvements with respect to the interim TFTP I agreement, such as:

    • The exclusion of SEPA data. The proposal explicitly foresees that requests from the US Treasury should not seek any data relating to the Single Euro Payments Area (Article 4.2.d)

    • The definition of terrorism. Article 2 of the proposal builds on the definition of terrorism on the approach of Article 1 of Council Framework Decision 2002/475/JHA[5].

11. In addition, further to the requests of the European Parliament and of European data protection authorities, the proposal lays down a series of provisions (Articles 14-18) dealing with data subjects' rights, such as the right to be informed, the right of access, the right to rectification, erasure or blocking, as well as the right to obtain redress. However, the concrete enforceability of these provisions and the procedures to be followed by non US citizens or residents are still not clear (see below paragraph II.2.3).

II.2 But further improvements are still needed

12. The EDPS fully shares the need to ensure, as envisaged by Article 1.1 of the proposal, full respect for the privacy and the protection of personal data. In this perspectives, the EDPS points out that there are still some open questions to address and key elements to improve in order to meet the conditions of the EU legal framework on the protection of personal data.

II.2.1 Is the envisaged processing of personal data really necessary and proportionate?

13. The EDPS is fully aware that the fight against terrorism and terrorism financing may require restrictions to the right to the protection of personal data as well as to

[5] Council Framework Decision of 13 June 2002 on combating terrorism, OJ L 164/3.

banking secrecy provisions. This is already the case in a series of EU instruments[6] containing a number of measures aimed at combating the misuse of the financial system for the purpose of money laundering and terrorist financing. These instruments also contain specific provisions allowing exchange of information with third countries authorities as well as safeguards for the protection of personal data, in line with Directive 95/46/EC.

14. Furthermore, the agreement on mutual legal assistance between the EU and the US explicitly allows the exchange between law enforcement authorities of information relating to bank accounts and financial transactions, and it provides conditions and limitations with regard to this exchange. Also at international level, the so-called Egmont Principles[7] set the basis for the international exchange of financial transactions information between Financial Intelligence Units, while establishing limitations and safeguards with regard to the use of exchanged data. In addition, instruments for the exchange of data between the US and Europol and Eurojust are already in place, ensuring at the same time exchange of information and protection of personal data.

15. Against this background, the Commission proposal highlights the usefulness of the TFTP Programme, as put forward by the US Treasury and by the eminent person's reports. However, the condition laid down by Article 8 ECHR in order to justify interference with private life is "necessity" rather than "usefulness".

16. According to the EDPS, sufficient evidence is needed of the real added value of this agreement taking into account already existing instruments, or, in other words, to which extent the agreement is really necessary in order to obtain results that could not be obtained by using less privacy-intrusive instruments, such as those already laid down by the existing EU and international framework. According to the EDPS, this added value should be unambiguously established, as a precondition for any agreement with the US on the exchange of financial data, also in view of the intrusive nature of the agreement (see also paragraphs 18-22 on proportionality).

17. The EDPS is not in a position to judge the necessity of this agreement. However, even if the necessity of the agreement is demonstrated, other points still deserve the attention of the negotiators.

18. Proportionality is also the main criterion when assessing the amount of personal data transferred and their storage period. Article 4 of the proposal narrows the scope of the US requests. However, the proposal still foresees that personal data will be transferred to the US authorities in bulk and then kept in principle for a period of 5 years irrespective of whether they have extracted or there is a proved link with a specific investigation or prosecution.

Bulk transfers

19. The proposal, in spite of the requests of the European Parliament and of the European data protection authorities, is still based on the concept that personal

6 In particular, Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds.

7 http://www.egmontgroup.org/library/download/5

data will be transmitted in bulk to the US Treasury. With regard to this point, it is important to clarify that the fact that the current SWIFT system does not allow a targeted search cannot be considered as a sufficient justification to make bulk data transfers lawful according to EU data protection law.

20. Therefore, EDPS believes that solutions should be found to ensure that bulk transfers are replaced with mechanisms allowing financial transaction data to be filtered in the EU, and ensuring that only relevant and necessary data are sent to US Authorities. If these solutions could not be found immediately, then the Agreement should in any event strictly define a short transitional period after which bulk transfers are no longer allowed.

Storage period

21. With regard to the storage period, the EDPS acknowledges that the proposal correctly establishes maximum retention periods as well as mechanisms to ensure that personal data are deleted when they are no longer necessary. However, the provisions of Article 6 of the proposal concerning non-extracted data seem to go in the opposite direction. First of all, the concept of "non-extracted data" is not self-evident and should thus be clarified. Secondly, the reasons for which it is necessary to keep non-extracted data for 5 years are not proved.

22. The EDPS fully acknowledges the need to ensure that personal data necessary for a specific anti-terrorism investigation or prosecution are accessed, processed and kept for as long as it is necessary, in some cases even beyond 5 years, as it may be the case that personal data are needed for long lasting investigations or judicial procedures. However, assuming that non-extracted data are data which have been transferred in bulk and which have neither been accessed nor used for a specific prosecution or investigation, the storage period allowed to keep these data should be much more limited. In this perspective, it is useful to highlight that the German Federal Constitutional Court has deemed that in the case of retention of telecommunications data, a storage period of 6 months is already very long and accordingly needs an adequate justification.[8] The Constitutional Court seemed to consider this 6 months period as a maximum for data that were not related to any specific investigation.

II.2.2 Does the proposal ensure judicial oversight?

23. According to the negotiating mandate, a judicial public authority should have the responsibility to receive the requests from the US Treasury, assess their compliance with the agreement and, where appropriate, require the provider to transfer the data on the basis of a "push" system. Both the European Parliament and the EDPS welcomed this approach, which represents a crucial guarantee - in line with national constitutions and legal systems of Member States - to ensure lawful and balanced transfers of data as well as independent oversight.

24. However, the proposal assigns this task to Europol, which is an EU Agency for the prevention and combat of organised crime, terrorism and other forms of serious

[8] Judgement of 2 March 2010.

crime, affecting two or more Member States.[9] It is obvious that Europol is not a judicial authority.

25. Moreover, Europol has specific interests in the exchange of personal data, on the basis of the proposed agreement. Article 10 of the proposal gives Europol the power to request for relevant information obtained through the TFTP, if it has a reason to believe that a person or an entity has a nexus to terrorism. It is hard to reconcile this power of Europol, which may be important for the fulfilment of Europol's task and which requires good relations with the US Treasury, with the task of Europol to ensure independent oversight.

26. Furthermore, the EDPS wonders to which extent the current legal framework entrusts Europol - especially without changing its legal basis pursuant to the ordinary procedure established by the Lisbon Treaty - with the tasks and powers to make an administrative request coming from a third country "binding" (Article 4.5) on a private company, which will thus become "authorized and required" to provide data to that third country. In this context it is useful to note that it is under the present state of EU law not evident whether a decision of Europol vis-à-vis a private company would be subject to judicial control by the European Court of Justice.

27. Against this background, the EDPS reiterates his position that, also with a view to respect the negotiating mandate and the current EU legal framework, the task to assess the requests of US Treasury should be entrusted to a public judicial authority.

II.2.3 Does the proposal confer enforceable data subjects' rights (and protection)?

28. As already mentioned in the introductory part of this opinion, the proposal lays down a series of data subjects' rights, such as the right to be informed, the right of access, the right to rectification, erasure or blocking, as well as the right to obtain redress. However, it is important on the one hand to improve some elements of these provisions, and on the other hand to ensure their effective enforceability.

29. With regard to the right to have access to one's own personal data, the agreement lays down a series of limitations. The EDPS acknowledges that, especially in the context of fight to terrorism, limitations to data subjects' rights may be put in place insofar as they are necessary. However, the proposal should make clear that, while disclosure to a person of his personal data may well be limited in the circumstances mentioned in Article 15.2, disclosure of this information to the European national data protection authorities should in all cases be possible, in order to allow these authorities to effectively fulfil their supervisory task. Of course, data protection authorities will be bound by a duty of confidentiality in performing their tasks and will not disclose the data to the person concerned, as long as the conditions for an exception subsist.

30. With regard to the right of rectification, Article 17. 2 states that "*Each Party shall, where feasible, notify the other if it becomes aware that material information it has transmitted to or received from the other Party under this Agreement is*

9 See, for instance, Article 3 of Council Decision 2009/371/JHA establishing the European Police Office (Europol), OJ L 121/37.

inaccurate or unreliable." The EDPS believes that the obligation to rectify inaccurate or unreliable data is a fundamental guarantee not only for the data subject, but also for the effectiveness of the action of law enforcement authorities. In this perspective, authorities exchanging data should put in place mechanisms to ensure that this rectification is always feasible, and the proposal should thus delete the words "*where feasible*".

31. However, the main concern of the EDPS relates to the concrete enforceability of these rights. On the one hand, for reasons of legal certainty and transparency, the proposal should specify in further details which are the concrete procedures that data subjects may use in order to enforce the rights recognised by the agreement, both in the EU and in the US.

32. On the other hand, Article 20.1 explicitly and clearly states that the agreement "*shall not create or confer any right or benefit on any person or entity, private or public*". The EDPS notes that this provision seems to annul or at least question the binding effect of those provisions of the agreement providing for data subjects' rights which are currently yet neither recognised nor enforceable under US law, in particular when data subjects are non US citizens or permanent residents. For example, the US Privacy Act provides a qualified right of access to personal information which is stronger than the general right of access granted to the general public by the US Freedom of Information Act. However, the US Privacy Act clearly states that a request for access to one's own records is only possible for "*a citizen of the United States or an alien lawfully admitted for permanent residence*".[10]

33. The EDPS therefore recommends that the current formulation of Article 20.1 should be revised in order to ensure that the rights conferred by the proposal are clearly stated and effectively enforceable also in US territory.

II.2.4 Does the proposal ensure satisfactory independent oversight and supervision?

34. Article 12 of the proposal lays down various levels of monitoring of the conditions and safeguards established by the agreement. "Independent overseers" will monitor in real time and retrospectively the searches put in place by the US Treasury. Furthermore, "an independent person appointed by the European Commission" will carry out an ongoing monitoring of the first level of oversight, including its independence. It should be clarified what the tasks of this independent person will be, how it will be guaranteed that he can actually fulfil his tasks and to whom he reports.

35. Article 13 also establishes a mechanism for a joint review, to be carried out after 6 months and then at regular intervals. This joint review will be carried out by a joint EU-US delegation, including for the EU delegation representatives of two data protection authorities, and will result in a report that the Commission will present to the European Parliament and the Council.

[10] This is confirmed by the information available on the US Treasury website "*When you make a request for notification of or access to records, it should: [...] State that you are a citizen of the United States or an alien lawfully admitted for permanent residence in the United States; [...]*", http://www.treas.gov/foia/how-to.html (last accessed on 21 June 2010).

36. The EDPS highlights that independent supervision is a key element of the right to the protection of personal data, as confirmed by Article 16 TFEU and Article 8 of the Charter of the Fundamental Rights of the Union. Recently, the Court of Justice established strict criteria for independence in its Judgement of 9 March 2010, Commission v. Germany[11]. It is obvious that the same strict criteria can not be imposed on third countries, but it is also clear that there can only be an adequate protection of personal data[12] in so far as there are sufficient guarantees for independent oversight. This is also a condition for international agreements with countries whose legal system does not establish the necessity of control by an independent authority.

37. Against this background, it is crucial that at least the modalities of the oversight and of the joint review, as well as the powers and the guarantees of independence of the persons involved in the oversight are clearly defined in the agreement rather than being "jointly coordinated" or determined at a later stage by the parties. In particular, it is important to ensure that both the person appointed by the European Commission and the representatives of European data protection authorities are put in a position to act independently and to effectively carry out their supervisory tasks.

38. Furthermore, the proposal should not only fix the date of the first joint review, to take place after 6 months, but also the timeline of the following review, that may for example take place every year thereafter. The EDPS also recommends to establish a link between the outcome of these joint reviews and the duration of the agreement.

39. In this context, the EDPS emphasises that a sunset clause is desirable, also in the light of the possible availability of more targeted solutions on the longer term. A sunset clause could also be a good incentive to ensure that the necessary efforts are put in the development of such solutions which would mean that there will be no reason any more for sending bulk data to he US Treasury.

40. In order to enhance the effectiveness of both the oversight and the joint review, information and relevant data should be available on the number of access and redress requests, possible follow-up (deletion, rectification, etc), as well as the number of decisions limiting rights of data subjects. In the same line, as far as the review is concerned, information should be available and reported on the quantity not only of messages "accessed" by the US Treasury but also of the messages "provided" to the US Treasury. This should be specified in the agreement.

41. Furthermore, the powers and competences of European data protection authorities should not be in any way limited by this proposal. In this perspective, the EDPS notes that the proposal makes a step back with respect to the interim TFTP agreement. Indeed, while the previous agreement stated in its preamble that "*this Agreement does not derogate from the existing powers of data protection authorities in Member States to protect individuals with regard to the processing of their personal data*", the proposal now refers to "*the supervision of competent data protection authorities in a manner consistent with the specific provisions of this agreement*". The EDPS therefore recommends that the proposal clearly states

11 Case C-518/07, nyr.

12 Article 10 of the proposed agreement states that the US Treasury is deemed to ensure an adequate level of protection.

that the agreement does not derogate or limit the powers of European data protection authorities.

III Conclusions

42. The EDPS acknowledges that this proposal envisages certain substantial improvements with respect to the interim TFTP I agreement, such as the exclusion of SEPA data, a more limited definition of terrorism, and more detailed provisions on data subjects' rights.

43. The EDPS notes however that an essential prerequisite to the assessment of the legitimacy of a new TFTP agreement should be met. The necessity of the scheme must be established in relation to already existing EU and international instruments.

44. Would this be the case, the EDPS points out that there are still some open questions to address and key elements to improve in order to meet the conditions of the EU legal framework on the protection of personal data, such as:

- Ensuring that bulk transfers are replaced with mechanisms allowing financial transaction data to be filtered in the EU, and ensuring that only relevant and necessary data are sent to US Authorities
- Considerably reducing the storage period for non-extracted data
- Entrusting the task to assess the requests of the US treasury to a public judicial authority, in line with the negotiating mandate and the current EU legal framework
- Ensuring that the data subjects' rights conferred by the proposal are clearly stated and effectively enforceable also in the US territory
- Enhancing the independent oversight and supervision mechanisms, by:
    i. ensuring that the tasks and role of both the person appointed by the European Commission and the representatives of European data protection authorities are well defined and that they are put in a position to act independently and to effectively carry out their supervisory tasks;
    ii. ensuring that joint reviews take place regularly and that their outcome is linked to the duration of the agreement through a sunset clause
    iii. extending the information available to independent overseers and data protection authorities
    iv. avoiding that the agreement limits the powers of European data protection authorities
- Including a reference to this opinion in the preamble of the Proposal.

Done in Brussels, 22 June 2010

(signed)

Peter HUSTINX
European Data Protection Supervisor