

Legal Service

SJ-0066/10
KB/hr
D(2010)5811

Brussels, - 2 -02- 2010

LEGAL OPINION

This document is a confidential legal opinion within the meaning of Article 4 (2) of Regulation 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. The European Parliament reserves all its rights should this be disclosed without its authorisation.

Re: SWIFT - Conclusion of European Union/United States Agreement on Financial Messaging Data to Prevent and Combat Terrorism and Terrorist Financing (TFTP) - consent procedure - legal basis - legal situation if consent is refused - conformity with Parliament's resolution of 17 September 2009 - "intention not to derogate" - Parliamentary access to information on the implementation of the Agreement

Executive summary

1. The duty to inform Parliament "*at all stages of the [consent] procedure*" means that it must be informed in good time of the recommendations submitted by the Commission, the negotiating directives, the authorisation to sign the agreement negotiated, and any decision to provide for its provisional application, in order that it may seek to influence the content of the agreement;
2. By requesting Parliament's consent for the conclusion of the TFTP Agreement in conditions in which it was impossible for practical reasons for Parliament to react before the provisional application came into operation, the Council has in effect set Parliament a deadline in breach of the spirit of Article 218(6) TFEU, and undermined in part the legal effect and the practical impact of Parliament's decision in the consent procedure, in particular as regards its provisional application;

3. It is not necessary to cite Article 16(2) TFEU in the legal basis for the Decision concluding the Agreement;
4. Should the TFTP Agreement be rejected, neither Directive 95/46 nor Framework Decision 2008/977 would apply to any data transfers to the United States, while the Agreement on Mutual Legal Assistance would not apply in respect of SWIFT, which does not appear to be a "financial institution" as defined in European Union law; because such data transfers are not *a priori* in contravention of Article 16 TFEU, the Charter of Fundamental Rights, or Council of Europe Convention n° 108, any possible breaches would have to be examined on a case by case basis;
5. The Agreement takes up some but not all of the demands set out in Parliament's resolution of 17 September 2009 on the agreement then being negotiated;
6. Article 13 of the Agreement should be interpreted as not permitting any derogations from the laws of the United States, the European Union or the Member States;
7. Information on the implementation of the Agreement is of direct relevance to the negotiation and conclusion of the long-term Agreement foreseen in Article 15(4), and Parliament is therefore entitled to have access to such information.

I Introduction

1. By letter of 1 February 2010 (annex), Mr Juan Fernando LÓPEZ AGUILAR, chairman of the Committee on Civil Liberties, Justice and Home Affairs (hereinafter, "LIBE"), requested a legal opinion on certain aspects of the Agreement between the European Union and the United States of America to make available to the United States Department of the Treasury financial payment messaging data to prevent and combat terrorism and terrorist financing (hereinafter the "[TFTP] Agreement"). Parliament was requested on 25 January 2010 to give its consent to this Agreement, which was signed on 30 November 2009, in accordance with the Treaty on European Union prior to the entry into force of the Lisbon Treaty.
2. The matter is scheduled to be examined at the meeting of the LIBE committee on 4 February 2010, with a view to a possible vote in plenary on 8 or 9 February 2010.
3. It should be emphasised at the outset that the analysis of the relevant provisions of the Agreement, and European Union law generally, provided by the Legal Service is necessarily of a legal character, taking account in particular of the approach to the interpretation and evaluation of such provisions which has been adopted by the Court of

Justice.¹ Thus, for example, as regards the principle of proportionality, the judicial review test is that the provision must be "manifestly inappropriate" to the objective the act seeks to achieve in order for the Court to annul the act alleged to contravene this principle.² This fact should be taken into account in appreciating the differences between the assessments presented in the present opinion and those of non-judicial supervisory bodies such as the European Data Protection Supervisor and the Article 29 Committee.

II SWIFT and the TFTP: some basic factual background³

4. "SWIFT" is the Society for Worldwide Interbank Telecommunication. It is a private company in the form of a cooperative society with limited responsibility ("*s.c.r.l.*") under Belgian law, with around 8500 clients, of which approximately 7800 are financial institutions. It provides a secure messaging service for financial transactions.
5. SWIFT messages contain two types of data, traffic data and the message data. **Traffic data** are the information contained in the header or trailer of the message, such as the sending institution, the receiving institution, the type of message and the transfer history. It does not contain data relating to individuals. **Message data** refers to the internal content of the message, and does contain personal data such as the name, address and account number of the payer and payee. This latter data is also referred to, notably in Article 4(2) of the TFTP Agreement, as "identifying information". In general, SWIFT does not retrieve, use or disclose message data, though it carries out an automatic verification of their formal content, to ensure, for example, that the bank of destination is mentioned, the currency is specified etc. It may also retrieve message data at the request of the customer, in order to resolve technical problems with its messaging service, or on foot of a mandatory request from a competent public authority.
6. SWIFT stores copies of the messages it handles for a period of 124 days, after which these are destroyed and are hence no longer available for the purposes of investigation. It was learned in June 2006 that, in order to ensure the possibility of access to such messages beyond this timeframe, the Office of Foreign Assets Control, a division of the United States Treasury Department, had required SWIFT to hand over copies of certain messages. It was able to do so because one of SWIFT's two storage facilities was situated on American soil, which is no longer the case; at present, one of these facilities is located in a Member State and one in Switzerland. In practice, the Office of Foreign Assets Control requested SWIFT's records of transactions on the basis of common features such as dates, country of origin or destination and the type of standard message, at a point in its investigations where it was not yet possible to identify precisely the suspicious transaction. To a large extent, the action of the Office was intended to

¹ On the other hand, the Legal Service does not have any specific technical expertise as regards payment messaging services or the detailed practical operation of the TFTP.

² See, for example, Case C-310/04 *Spain v Council* [2006] ECR I-7285, paragraph 99.

³ This background information has been gleaned from the Decision of the Belgian *Commission de la Protection de la Vie Privée* of 9 December 2008 and various documents published by SWIFT, unless the contrary is indicated.

conserve evidence of terrorist conduct or terrorist financing, which could then be searched at a later stage in the investigation on the basis of more precise information obtained subsequently.

7. The manner in which SWIFT data are handled in the framework of the TFTP was described as follows in the 2007 "Representations" of the United States Treasury Department to the Council and the Commission:

*"SWIFT is required to provide only data the Treasury Department believes will be necessary in combating terrorist financing, on the basis of past analyses focusing on message types and geography, as well as perceived threats and vulnerabilities. Additionally, searches are narrowly tailored to minimize the extraction of messages that are not relevant to a terrorism investigation. The data provided by SWIFT are searched to extract only information that is related to an identified, pre-existing terrorism investigation. This means that every search that is conducted must specifically cite to (sic) and record documented evidence supporting the belief that the target is connected with terrorism or its financing. Each and every search of the SWIFT data under the TFTP is also logged contemporaneously, including such affirmative terrorism nexus required to initiate the search. As a result of the foregoing safeguards, only a minute fraction (i.e. substantially less than one percent) of the subset of SWIFT messages furnished to the Treasury Department has been actually accessed, and only because those messages have been directly responsive to a targeted terrorism-related search".*⁴

8. These Representations are in turn cited in the eighth recital in the preamble to the Agreement as being *"the rigorous controls and safeguards utilised by the U.S. Treasury Department"*. In so far as they are not reflected in the corpus of the Agreement, the United States would not be prevented from modifying them; however, as part of the context in which the Agreement was negotiated, at the very least, the United States would be obliged to notify to the European Union of any modification of these controls and safeguards.

III Procedure – Parliamentary participation

9. The TFTP Agreement is to be concluded in accordance with Article 218 TFEU. Parliament's participation in the procedure for the conclusion of agreements such as the TFTP Agreement comprises at least the following four elements:
 - Parliament is to be *"fully and immediately informed at all stages of the procedure"*;
 - Parliament may give or refuse its consent to the proposed agreement;
 - it may *"in an urgent situation, agree [with the Council] upon a time-limit for consent"*;

⁴ OJ 2007 C 166/17 to 27.

- Parliament, in common with the Council, the Commission and the Member States, may, prior to deciding on consent, request an opinion from the Court of Justice as to the compatibility of the envisaged agreement with the Treaties.⁵
10. The *ratio legis* of such a duty to inform is not to allow Parliament passively to take note of the actions of the other institutions, but to afford it the opportunity of bringing some influence to bear on the Commission and the Council as regards the content of the agreement, in order to facilitate its consent on the final text. It is firstly a reflection of the "*fundamental democratic principle that the peoples should take part in the exercise of power through the intermediary of a representative assembly*", to which the Court first referred in the 1963 landmark judgment in *Van Gend en Loos* and on which it has subsequently relied in a number of other major institutional cases.⁶ This principle has been significantly reinforced by the Lisbon Treaty amendments to the Treaty on the European Union, and particularly the new provisions on democratic principles of Articles 9 to 12 TEU, which must be considered relevant for the interpretation of the procedural articles of the TFEU. It follows that the procedural provisions of Article 218 TFEU should be scrupulously observed.
 11. The duty of parliamentary information is, moreover, a reflection of the more general duty on the institutions to "*practice mutual sincere cooperation*" set out in Article 13(2) TEU, which should equally inform the interpretation of the procedural provisions of the Treaty if these are not to be an empty formality. Should Parliament have any fundamental objections to an agreement for which its consent is required, it is in the interests of all the parties concerned that Parliament be given the opportunity to voice these as early as possible in the negotiation procedure.
 12. It follows that parliamentary consent should not be reduced to a take-it-or-leave-it decision on an agreement presented to it as a *fait accompli* some months after it has been signed and a week before its provisional application.⁷ The duty to inform Parliament at *all* stages of the procedure means that it must be informed in good time of the recommendations submitted by the Commission, the negotiating directives, the authorisation to sign the agreement negotiated, and any decision to provide for its provisional entry into force.
 13. By signing an agreement which provides for its provisional application from 1 February 2010, and then requesting Parliament on 25 January 2010 to give its consent, at a time when for practical reasons it was impossible for Parliament to react before 1 February 2010, the Council has in effect set Parliament a deadline, in breach of the spirit of

⁵ Respectively Article 218(10), (6)(a) and (11).

⁶ Case 26/62 [1963] ECR I, 12, Case 178/79 *Roquette Frères v Council (Isoglucose)* [1980] ECR 3333, paragraph 34, and Case C-300/89 *Commission v Council (Titanium dioxide)* [1991] ECR I-2867, paragraph 20.

⁷ The fact that the services of the Commission were allowed over five working weeks from the signature of the Agreement to complete the translation of a text of less than five and a half pages in the *Official Journal*, while Parliament was put into a position where it has to decide, at least on whether or not to take a decision on consent, in a significantly shorter period, has been amply commented on.

Article 218(6)(a) TFEU which requires Parliament's agreement for such a deadline.⁸ Moreover, the legal effect and the practical impact of any decision Parliament may take after 31 January 2010 to refuse consent would be significantly undermined by the fact that the Agreement will already have been applied provisionally from 1 February 2010.

14. In a letter to the President of the European Parliament, Mr Jerzy BUZEK, of 26 January 2010, the President of the Spanish Government, Mr José Luis RODRÍGUEZ ZAPATERO, declared that "[the] *provisional application* [of the Agreement] *in no way affects the prerogatives of the European Parliament*". However, because of the extremely late request for consent, the Council has put Parliament in a position where it must either accept the Agreement, including its provisional application, and renounce the possibility of properly exercising of its prerogatives, or reject the Agreement and thereby abolish rights which have already been applied, which could create legal uncertainty and undermine the credibility of the European Union on the international stage.
15. The provisional application of the Agreement also allows the United States to present an unlimited number of requests for data immediately as from 1 February 2010, which in accordance with Article 4(5), third subparagraph, of the Agreement, must be "*executed as a matter of urgency*", without regard to Parliament's view on whether the Agreement is acceptable or not.
16. In the circumstances of the present case, it does not necessarily follow, however, that the Council acted illegally in signing the present Agreement, or that Parliament's consent to the conclusion of the Agreement would necessarily be vitiated by a procedural defect. Absent any indication to the contrary, the Agreement may be considered to be legally valid when it was signed.⁹

IV Question 1: The legal basis of the Decision to conclude the Agreement

17. The first question put by Mr López Aguilar reads as follows:

Should the legal basis of the proposal for a Council Decision on the conclusion of the above-mentioned agreement also refer explicitly to Article 16 TFEU (data protection) and the now binding Charter of Fundamental Rights?

18. The draft of the Council Decision for the conclusion of the Agreement cites Article 82(1)(d) TFEU and Article 87(2)(a) TFEU as the "internal" legal basis, that is, the source of material competence, and Article 218(6)(a) TFEU as the procedural legal basis, which provides for Parliament's consent.

⁸ Parliament was obliged to react in a similar timeframe on the proposed EU-US Agreements on extradition and mutual legal assistance in 2003, as the Council declassified the texts just under a month before they were signed. Parliament's opinion, still less its consent, was not required under the procedure applicable.

⁹ See, for example, the Legal Opinion of 27 August 2009, SJ-398/09, concerning the legal basis.

19. Article 82(1)(d) TFEU provides the Union with competence to "*facilitate cooperation between judicial or equivalent authorities of the Member States in relation to criminal matters*", while Article 87(2)(a) TFEU allows for "*the collection, storage, processing, analysis and exchange of relevant information*". There is no reason to contest the relevance of these articles as part of the legal basis in the present note. The question raised in the letter from Mr López Aguilar is essentially whether Articles 82(1) and 87(2)(a) TFEU are sufficient as a legal basis for the conclusion of the Agreement, or whether it is also necessary as a matter of law to add a reference to Article 16 TFEU.
20. In accordance with the case-law of the Court of Justice, if the measure pursues a twofold purpose of which one can be identified as the main or predominant purpose, whereas the other is merely incidental, the act must be based on a single legal basis. Exceptionally, if the act simultaneously pursues a number of objectives or has several components that are indissociably linked, without one being secondary and indirect in relation to the other, the act will have to be founded on the various corresponding legal bases.¹⁰ Where it is not disputed that the act pursues one objective, a second legal basis is only required where the act pursues a second objective and contains components falling within another policy which are of such importance that the act ought to have a dual legal basis.¹¹
21. The purpose of the Agreement is defined in the first recital in the preamble as being "*to prevent and combat terrorism and its financing*", a purpose which is to be achieved through making available to the United States authorities certain financial data. While it is true that the means of carrying out this objective require "*full respect for the privacy, protection of personal data, and other conditions set out in [the] Agreement*" (Article 1(1)), it could be argued that, having regard to Article 16(1) TFEU and the relevant provisions of the Charter on Fundamental Rights, Article 82(1)(d) TFEU and Article 87(2)(a) TFEU are in any case sufficient as a legal basis for the conclusion of the Agreement, without it being necessary to cite Article 16(2) TFEU expressly. In particular, in allowing the Union to "*establish measures concerning the ... exchange of relevant information*" for the "*prevention, detection and investigation of criminal offences*", Article 87(2)(a) TFEU necessarily implies a power to adopt the rules on data protection which will allow the Union to comply with its duties in this regard.
22. It follows that it is not necessary to cite Article 16(2) TFEU in the legal basis.

¹⁰ Case C-166/07 *Parliament v Council*, judgment of 3 September 2009, paragraphs 46 and 47.

¹¹ *Ibid.* paragraph 48.

V Question 2: The legal situation should the TFTP Agreement be rejected

23. The second question put by Mr López Aguilar reads as follows:

Should the European Parliament refuse to give its consent, under what conditions and safeguards could the US obtain information covered by this EU-US agreement from the Member States?

24. If Parliament refuses consent, the TFTP Agreement would not enter into force and the provisional application thereof would terminate upon notification by the European Union to the United States authorities.¹² It remains to be considered which provisions of European Union law might then be applicable to transfers of data to the United States Treasury Department.

(a) *The internal market Directive and Framework Decision*

25. Neither Parliament and Council Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data nor Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter would apply to any transfers of data effected by SWIFT on request of the United States authorities.¹³ Article 3(2) of the Directive provides explicitly that it does not apply to processing of personal data outside the scope of what was then Community law, nor to processing operations in the field of public security or criminal law enforcement. The Member States are only obliged to ensure compliance with the Framework Decision as from 27 November 2010.

(b) *The European Union–United States Agreement on Mutual Legal Assistance*

26. The European Union–United States Agreement on Mutual Legal Assistance which came into force on 1 February 2010 is a much more general instrument than the TFTP Agreement. For those Member States which have a bilateral agreement with the United States on mutual legal assistance, the Agreement on Mutual Legal Assistance supplements, rather than replaces, the bilateral agreement. This Agreement is not limited to terrorist offences; as regards requests for bank information, it is sufficient that the request concern “*an identified natural or legal person suspected of or charged with a criminal offence*”, though the State may restrict the categories of offences in respect of which it will provide assistance.¹⁴ The information may include records of specified bank “accounts or transactions” in the possession of banks or non-bank financial institutions.¹⁵ The information request must, in particular, identify the person, indicate

¹² See Article 25(2), Vienna Convention on the Law of Treaties between States and International Organisations and the equivalent provision of the Vienna Convention on the Law of Treaties.

¹³ Respectively OJ 1995 L 281/31 and OJ 2008 L 350/60. For the avoidance of doubt, Regulation 45/2001 does not apply because it only governs the processing of personal data by the Community institutions, not by private companies.

¹⁴ Article 4(1)(a) and (4).

¹⁵ Article 4(6).

the grounds for suspecting he has committed a crime and show how the information relates to the criminal investigation or proceeding.¹⁶

27. The term "non-bank financial institution" is not defined in the Mutual Legal Assistance Agreement. However, SWIFT is essentially a telecommunications company and, while it arranges for the transmission of financial data, it seems unlikely that it could be considered a "financial institution". Directive 2005/60/EC on money laundering, which applies to "financial institutions", expressly excludes from its scope of application "*any natural or legal person that provides credit or financial institutions solely with a message or other support systems for transmitting funds or with clearing and settling systems*".¹⁷ It could be argued by analogy that SWIFT is not therefore a financial institution.
28. Moreover, even if SWIFT could be considered to come within the scope of the Mutual Legal Assistance Agreement, access to bank information is only allowed in situations in which a criminal offence has already been committed, and requests concerning accounts and transactions specified in the request, whereas the TFTP Agreement allows requests for preventive purposes, and without necessarily identifying at this stage an accused person.
29. It should also be noted that the data protection provisions of the Agreement on Mutual Legal Assistance Agreement are significantly less developed than those of the TFTP.¹⁸ While national provisions may be applicable, the Member State is nonetheless obliged, as a matter of European Union law, to give precedence to its obligations under the Agreement in case of inconsistency. Thus the Mutual Legal Assistance Agreement between the United States and the Netherlands, to take the rapporteur's home Member State, provides that requests from the United States authorities "*shall be executed according to [Netherlands] domestic law and procedures ... except to the extent that this Treaty provides otherwise*".¹⁹

(c) *Article 16 TFEU and the Charter of Fundamental Rights*

30. Article 16(1) TFEU provides that "[everyone] has the right to the protection of personal data concerning them". While *prima facie* this has the character of a fundamental right in European Union law, fundamental does not mean absolute. The fact that persons have a right to the protection of their personal data does not preclude processing for legitimate purposes, processing which is for the most part in the interests of the data subject. It is open to doubt that this provision could successfully be relied upon in a court of law, in the sense of having direct effect in Union law, as its application *prima facie* requires some measure of implementation on the part of the Member State concerned.

¹⁶ Article 4(2).

¹⁷ Recital 34 in the preamble and Article 2(1)(2), OJ 2005 L309/19; the preamble to Regulation 1781/2006 on information on the payer accompanying transfers of funds contains a similar recital (OJ 2006 L345/1).

¹⁸ Resolution of 3 June 2003, P5_TA(2003)0239.

¹⁹ Article 12(2), 27 Tractatenblad (2004) n°1.

31. Personal data is also protected in accordance with Article 8 of the Charter of Fundamental Rights of the European Union, which now has the same status as other provisions of the Treaty. Article 8(2) that "[such] data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". Articles 7, 47, 48 and 49 of the Charter have also been mentioned in this regard.
32. Assuming for the purposes of argument that the Member State is bound by these provisions,²⁰ the rights granted are nonetheless subject to the general qualifications of Article 52 of the Charter, which allows limitations on Charter rights "[subject] to the principle of proportionality ... if they are necessary and genuinely meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". In legal terms, it cannot be concluded without a full examination of the legal and factual context, and the justification relied on for the transfer of data and any other action complained of, that these would necessarily contravene the specified Charter rights.
33. The European Union institutions are in any case bound by Article 16(1) TFEU and the Charter in taking a decision on the conclusion of the TFTP Agreement. It could possibly be argued that in allowing the transfer of data to the United States, the Agreement fails to respect the principle of proportionality. As against this, it appears that the purposes for which the Agreement has been drawn up are consistent with those of the Treaties, and that certain safeguards have been foreseen. In order to prove that the Agreement is invalid as a matter of European Union law, it would have to be demonstrated that the means employed by the Agreement are "*manifestly inappropriate*" to the achievement of those objectives.²¹ It is not possible for the Legal Service to take a useful position on this question in the abstract, or to show how the same ends could be achieved by less data-intrusive means.

(d) *European Convention on the Protection of Human Rights*

34. Article 8 of the European Convention for the Protection of Human Rights (ECHR) provides for the respect for private life. The right to privacy must be balanced with other interests, such as law enforcement. Member States can take privacy or personal data-intrusive measures upon condition that these are necessary for the enforcement of criminal law. Article 8(2) of the ECHR specifies that there shall be no interference by a public authority with the exercise of the right of privacy (including the protection of personal data) unless the interference is in conformity with the law and is necessary in a democratic society for the protection of public order and the prevention of crime.

²⁰ If the TFTP Agreement is rejected, the Member State transferring data to the United States would not be "implementing Union law" within the meaning of Article 51(1) of the Charter, but could be said to acting within the scope of Union law (see Legal Service note SJ-527/09 of 27 November 2009 on the Charter of Fundamental Rights, paragraph 6).

²¹ See, for example, Case C-310/04 *Spain v Council* [2006] ECR I-7285, paragraph 99.

Member States have a certain margin of appreciation in adopting and implementing internal rules in accordance with the principles of the ECHR.

35. In addition, any restriction on the right to privacy and to protection of personal data must be based on law. The European Court of Human Rights refers to one formal requirement, that is to say the existence of a domestic law, and to one substantive requirement, that is to say the quality of the law in dispute, which has to be compatible with the rule of law.²² The law in question must be both accessible and foreseeable as to its effects.²³
36. The European Court of Human Rights also requires that any interference justified in accordance with Article 8(2) ECHR respect the principle of proportionality. In the present case, the question is whether the treatment and transfer of SWIFT data by a Member States would exceed what is necessary to achieve to objective of fighting terrorism and terrorist financing. Again, without a full examination of the legal and factual context, and the justification relied on for the action complained of, it cannot be concluded that this would necessarily contravene Article 8 of the Convention.

(e) *Council of Europe Convention 108*

37. All the Member States are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981 (Convention 108). The principles it establishes may be considered as the most authoritative statements of general principles governing the protection of personal data.
38. Articles 5, 6 and 8 of the Convention lay down a number of substantive rules on the protection of personal data. However, Article 9(2) expressly allows derogations from these provisions which are necessary in a democratic society either to protect certain interests, including the protection of State security and the suppression of criminal offences, or to protect the data subject or the rights and freedoms of others. Once again, it cannot be concluded without a full examination of the legal and factual context, and the justification for the transfer of data relied on that this would necessarily contravene Convention 108.
39. By way of response to Question 2, the Legal Service is of the opinion that if the TFTP Agreement is not concluded, the transfer of data to the United States will be governed by the domestic law of the Member State(s) concerned, subject to any demonstrable breach in an individual case of the provisions of European Union law outlined above.

²² Judgment of 2 August 1984, in *Malone v United Kingdom*, paragraph 87.

²³ Judgment of 26 April 1979, in *Sunday Times v United Kingdom*, paragraph 49.

VI Question 3: Conformity of the Agreement with resolution of 17 September 2009

40. Mr López Aguilar's third question is:

To what extent are the provisions of the EU-US TFTP interim agreement in line with the European Parliament resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing, notably paragraphs 2, 7, 8 and 11?

41. In the first place, it should be pointed out that a resolution of the European Parliament adopted at its own initiative is not a legally binding act which could be employed as a standard for the legality of an act of European Union law. In the present circumstances, the question may read as a request to identify and assess the relevant provisions of the TFTP Agreement in the light of the corresponding paragraphs of the resolution.

(a) Paragraph 2 of the resolution

Stresses that the European Union is based on the rule of law and that all transfers of European personal data to third countries for security purposes should respect procedural guarantees and defence rights and comply with data-protection legislation at national and European level²⁴;

42. The provisions of European Union law governing data protection have been examined at answering Question 2 above. If concluded, the TFTP Agreement would be binding, as a matter of European Union law, on the Member States, the application of whose "procedural guarantees and defence rights and data-protection legislation" would therefore be subject to compliance with the Agreement.²⁵ That said, the fifth recital in the preamble to the Agreement notes that the transfer of data may only take place "subject to strict compliance with safeguards on privacy and the protection of personal data", a concern reflected in a number of other provisions of the Agreement, such as the first sentence of Article 1(1), Article 4(2), and Article 5.

(b) Paragraph 7 of the resolution

[The European Parliament believes], to the extent that an international agreement is absolutely necessary, that it must as a very minimum ensure:

(a) *that data are transferred and processed only for the purposes of fighting terrorism,*

²⁴ Notably the European Convention on Human Rights, in particular Articles 5, 6, 7 and 8 thereof, the Charter of Fundamental Rights, in particular Articles 7, 8, 47, 48 and 49 thereof, Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Directive 95/46/EC and Regulation (EC) No 45/2001.

²⁵ Article 4(5), first subparagraph, provides that data transfers are to be executed "under the law of the requested Member State".

- Purpose limitation

43. Article 1(1)(a) of the Agreement provides for the making available of "*financial payment messaging and related data ... for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing*". The same purpose limitation is reflected in Articles 3, 4(1), 4(2) and 4(5) of the Agreement.
44. The conditions under which processing can take place are defined in Article 5; in particular, Article 5(2)(c) provides that "[*each*] *individual TFTP search of Provided Data shall be narrowly tailored, shall demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing*".

as defined in Article 1 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism,

- Definition of "terrorism"

45. Article 2 of the TFTP Agreement provides a definition of terrorist conduct which is in most respects substantially identical to that in the Framework Decision.²⁶ Both involve acts of violence or danger to human life, property or infrastructure committed with the aim of intimidating, coercing or destabilising a population, government or international organisation, or action which assists or attempts to commit such acts.
46. It is true that the Framework Decision requires that the terrorist act be an offence in national law, and then provides a list of nine categories of acts which are to be deemed "terrorist offences", whereas the Agreement refers only to "acts".²⁷ It may be that the Agreement would cover requests for data with a view to the prevention (etc.) of acts which are not included in the Council list, though, given its extensive scope, the significance in practical terms would need to be demonstrated. It should also be noted that in one respect the Council definition is wider, in that, unlike the Agreement, it covers "*threatening to commit any of the acts*" listed.²⁸

- Limitation of requests to those concerning "*individuals or terrorist organisations recognised as such also by the EU*"

47. The TFTP Agreement is based on requests for data concerning conduct rather than requests concerning people or organisations whom/which are identified in advance. Article 4 provides that requests must be "*based on an ongoing investigation concerning a specific conduct*" defined as terrorist "*that has been committed or where there is, based on pre-existing information or evidence, a reason to believe that it could be committed*". Article 8 of the Agreement on Mutual Legal Assistance, to which Article 4 of the TFTP Agreement refers, specifies that an administrative authority, such as the US

²⁶ OJ L 164, 22.6.2002, p. 3.

²⁷ Article 1(1)(a) to (i) of the Framework Decision, Article 2(a) of the Agreement.

²⁸ Article 1(1)(i) of the Framework Decision.

Treasury Department, may only request information when "*investigating conduct with a view to a criminal prosecution of that conduct, or referral of the conduct to criminal investigation or prosecution authorities*".

48. Data searches, on the other hand, are based on requests regarding identified persons or entities. Thus, under Article 5(2)(c), "*[each] individual TFTP search of Provided Data shall be narrowly tailored, shall demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing, and shall be logged, including such nexus to terrorism or its financing required to initiate the search*". That said, the Agreement does not require that either data transfer requests or searches concern persons or organisations previously identified at the European Union level as being involved in terrorism or terrorist financing.
- Scope of data requests
49. Article 2 of the Agreement defines the scope of the Agreement as being "*the obtaining and use of financial payment messaging and related data*", without providing a precise indication of what is intended by "related data". However, Article 4(2) specifies that the data which may be requested includes both "*identifying information about the originator and/or recipient of the transaction ... and other personal data related to financial messages*". It is clear that the purpose limitation of Article 1(1)(a) of the Agreement applies to all types of data and the transmission and processing of such related data may only take place "*with full respect for the privacy, protection of personal data and other conditions set out in [the] Agreement*".
 - (b) *that the processing of such data as regards their transfer (only by means of a 'push' system), storage and use is not disproportionate to the objective for which those data have been transferred and are subsequently processed;*
50. The data which is requested under Article 1(1)(a) of the Agreement is to be "*made available upon request*", which indicates the so-called "push system".
51. The principal conditions for the use of data transmitted to the U.S. are set out in Article 5 of the Agreement. This provides:
 - purpose limitation on processing and sharing data ("*exclusively for the prevention, investigation, detection, or prosecution of terrorism or its financing*");
 - requirements that the subject of the search have a demonstrable "*nexus to terrorism or its financing*" and that the search be "*narrowly tailored*" in consequence
 - rules on the secure physical storage and restricted physical access to the provided data
 - review and deletion within specified deadlines of non-extracted data and data transmitted in error;
 - retention of information extracted from provided data in accordance with the retention periods of the particular government authority.

52. The assessment from the legal point of view of whether the arrangements set out above are proportional to the achievement of that objective is to a large extent a question of fact; the party seeking to demonstrate a breach of the principle of proportionality must show that the same ends can be achieved by less intrusive means. Moreover, as note above, the judicial review test is that the provision must be "manifestly appropriate" for the Court to annul it.²⁹ The Legal Service does not dispose of the necessary information to come to a considered view on this matter.

(c) *that the transfer requests are based on specific, targeted cases,*

53. As noted above, transfer requests must in accordance with Article 4(1) of the Agreement be "*based on an ongoing investigation concerning a specific [terrorist] conduct ... that has been committed*" or is likely to be committed.

limited in time and subject to judicial authorisation,

54. The Agreement does not expressly provide that transfer requests be limited in time. The requested Member State is nonetheless required to comply with a valid request "*as a matter of urgency*";³⁰ this requirement should ensure that, as a matter of practice, requests are limited in time.

55. Equally, the Agreement does not expressly provide that transfer requests be subject to judicial authorisation. Article 4(3) provides that the request be transmitted to the "*central authority of the Member State*" concerned, and it is therefore a matter for that State to decide whether or not this is to be an administrative or judicial authority. Where the law of that Member State provides for a prior judicial authorisation for the data transfer, this requirement must be complied with.

and that any subsequent processing is limited to data which disclose a link with persons or organisations under examination in the US;

56. Article 4(9) of the Agreement provides that "[the] *data that have been transmitted lawfully on the basis of this provision may be searched for the purpose of other investigations concerning the types of conduct referred to in Article 2, with full respect for Article 5 of this Agreement.*" As noted above, data requests must be connected with "*an ongoing investigation concerning a specific conduct*".

that data which do not disclose such links are erased;

57. Article 5(2)(i), (k) and (l) provides for the erasure of all non-extracted data after a specified period. However, the information extracted "*shall be subject to the retention period applicable to the particular government authority according to its particular regulations and record retention schedules*". The text of the Agreement provides no

²⁹ See, for example, Case C-310/04 *Spain v Council* [2006] ECR I-7285, paragraph 99.

³⁰ Article 4(5), third paragraph, of the Agreement.

indication of what these retention periods are, or of whether and when data which is extracted but found not to contain usable information is to be erased.

(d) *that EU citizens and enterprises are granted the same defence rights and procedural guarantees and the same right of access to justice as exist in the EU and that the legality and proportionality of the transfer requests are open to judicial review in the US;*

58. The question of redress within the European Union is dealt with in Article 11(1), which allows a data subject to request his or her data protection authority to confirm “*whether all the necessary verifications have taken place ... to ensure that his or her data protection rights have been respected*”, subject to any “*necessary and proportionate measures applicable under national law for the protection of public security or national security*” or in the interests of law enforcement.

59. Given the fact that most data requested is not in fact searched, it seems likely that any problems which arise for individuals or companies in this regard would do so in respect of action taken on foot of such a search, rather than the transfer request *per se*.

60. The Agreement does not guarantee European citizens and companies the same rights and guarantees under United States law as they would enjoy in the territory of the European Union, and indeed given the difference between legal systems both within the European Union and the United States, and between the jurisdictions concerned, this would cause significant practical problems. Instead, the Agreement guarantees “*effective administrative and judicial redress in accordance with the law ... of the United States*” (Article 11(3)). The 2007 Representations describe various forms of independent oversight of the activities of the Treasury Department in respect of transferred data, and notes that the limited nature of the data concerned, the restricted access thereto and the limits on dissemination thereof “*significantly reduce the pertinence of a redress mechanism*”.³¹ They also provide an illustration of the possibilities for redress to challenge administrative action, including administrative reconsideration and judicial review under the Administrative Procedure Act. Neither the Agreement nor the Representations indicate under what circumstances an individual or company outside the territory of the United States is to be informed of the fact that an unfavourable decision has been taken in regard to him/it on the basis of extracted data.

(e) *that transferred data are subject to the same judicial redress mechanisms as would apply to data held within the EU, including compensation in the event of unlawful processing of personal data;*

61. The transfer of data to the US authorities takes place within the territory of the EU, and is therefore, as regards the actual transfer, the same judicial redress mechanisms should apply as would in respect of a transfer from one Member State to another or within a single Member State. The redress mechanisms in force within the United States have been outlined in the previous paragraph.

³¹ Cited above, page 23.

- (f) *that the agreement prohibits any use of SWIFT data by US authorities for purposes other than those linked to terrorism financing*
62. As noted above, Article 4(9) of the Agreement provides that "[the] data that have been transmitted lawfully on the basis of this provision may be searched for the purpose of other investigations concerning the types of conduct referred to in Article 2, with full respect for Article 5 of this Agreement." This provision seeks to ensure that SWIFT data may only be used for the investigation of terrorist conduct.
- and that the transfer of such data to third parties other than the public authorities in charge of the fight against terrorism financing is also prohibited;*
63. The Agreement does not provide for the transfer of SWIFT data to third parties. Instead, Article 5(2)(h) allows the sharing with "law enforcement, public security, or counter-terrorism authorities in the United States, European Union, or third States to be used for the purposes of the investigation, detection, prevention, or prosecution of terrorism or its financing" of "terrorist leads". While the term "lead" is a colloquialism not commonly found in formal provisions of European Union law on criminal cooperation, the sense is clear, that is, an indication intended to assist the law enforcement authorities investigate, detect, prevent or prosecute terrorism or terrorist financing.
- (g) *that a reciprocity mechanism is strictly adhered to, obliging the competent US authorities to transfer relevant financial messaging data to the competent EU authorities, upon request;*
64. True reciprocity would require the United States authorities to allow the authorities of the European Union to obtain and use financial payment messaging and related data stored in servers in the United States. However, no such European Union authority currently exists. If it were to be established, Article 9 of the Agreement would require the United States Treasury Department to "actively pursue, on the basis of reciprocity and appropriate safeguards, the cooperation of any relevant [United States] service providers."
65. In the meantime, Article 8 allows any competent Member State authority, Europol and Eurojust to obtain information from the Treasury Department on request, while Article 7 requires the Treasury Department on its own initiative to make available to the authorities of the Member States concerned TFTP information "that may contribute to the investigation, prevention, detection, or prosecution in the European Union of terrorism or its financing".
- (h) *that the agreement is expressly set up for an intermediate period by means of a sunset clause not exceeding 12 months,*
66. The Agreement is valid until 31 October 2010 at the latest (Article 15(3)).

and [be] without prejudice to the procedure to be followed under the Lisbon Treaty for the possible conclusion of a new agreement in this field;

67. In legal terms, the Agreement of 30 November 2009 does not prejudice the procedure for the adoption of a definitive Agreement. Moreover, the twelfth recital in the preamble declares that the Agreement "*does not constitute a precedent for any future arrangements between the United States and the European Union*" in this area.

(i) *that the interim agreement clearly provides for the US authorities to be notified forthwith after the entry into force of the Lisbon Treaty and that a possible new agreement will be negotiated under the new EU legal framework that fully involves the European Parliament and national parliaments;*

68. Article 15(4) provides that "[as] soon as the Treaty of Lisbon enters into force, the Parties shall endeavour to conclude a long-term agreement to succeed this Agreement". In order to implement the European Union's obligations under this provision, the Commission is under a duty to initiate the procedure for the negotiation and conclusion of a definitive agreement.

69. The Agreement does not expressly provide that the "*possible new agreement will be negotiated under the new EU legal framework*", as such a provision would be otiose.

(c) Paragraph 8 of the Resolution

Requests the Council and the Commission to clarify the precise role of the 'public authority' to be designated with responsibility to receive requests from the US Treasury Department, taking into account in particular the nature of the powers vested in such an 'authority' and the way in which such powers could be enforced;

70. Article 4(3) of the Agreement requires the United States Treasury Department to address its requests for access to SWIFT data to "*the central authority of the Member State*" concerned. As noted above, the designation of that authority is a matter for the Member State, on which it would not be appropriate for the Agreement to lay down any more specific provision. The Legal Service has not been informed whether or not Parliament or the LIBE committee has received such clarification.

(d) Paragraph 11 of the Resolution

Underlines the importance of legal certainty and immunity for citizens and private organisations subject to data transfers under such arrangements as the proposed EU-US agreement;

71. As regards legal certainty, the provisions of European Union law apart from the TFTP Agreement itself which may be relevant to data transfers have been examined above. As the United States Treasury Department has pledged only to request and use such data in

connection with investigations of (planned) acts of terrorism or terrorist financing, it is somewhat difficult to see what "*immunity for citizens and private organisations*" is intended.

VII Question 4: Article 13 of the Agreement and the intention not to derogate

72. The fourth question put by Mr López Aguilar is as follows:

What is the exact meaning of Article 13 which underlines that 'the Agreement is not intended to derogate from or amend the laws of the United States or the European Union or its Member States'? Should it be understood then that the final rule applicable as regards the transfer of data is the national legislation of the requested Member State?

73. According to Article 13, "[*this*] Agreement is not intended to derogate from or amend the laws of the United States or the European Union or its Member States". The expression "intended not to derogate" does not correspond to any term of art in European Union law. On the literal level, it could be interpreted to mean that the Agreement sanctions any derogations which occur, but that these are to be interpreted in such a manner as to keep their impact to a minimum. Alternatively, it could be interpreted as meaning that the Agreement may not derogate from the laws listed.
74. The general principle of law is that derogations should not be assumed and in the absence of a clear indication in the text of the Agreement that it allows any derogations, it could be argued that none is permitted. This interpretation is supported by the sixth recital in the preamble by which both parties to the Agreement acknowledge that the European Union is bound to respect the fundamental rights and principles mentioned, and the thirteenth recital, which recognises that the Agreement "*does not derogate from the existing powers of data protection authorities in the Member States to protect individuals with regard to the processing of their personal data*". This interpretation would also be consistent with the Declaration made by the European Union at the time of the signing of the Agreement which notes that "[*the*] Agreement, while not derogating from or amending the legislation of the European Union or its Member States" will be provisionally implemented by the Member States in accordance with their national laws (including, presumably, any applicable provisions of European Union law).
75. In any case, both the European Union and the Member States are obliged to "*take all necessary and appropriate measures within their authority to carry out the provisions and achieve the purpose of [the] Agreement*", including, as regards the transfer of data from the territory of the European Union, the provisions of the Agreement concerning data protection. As noted above, Article 4(5), first subparagraph, of the Agreement provides that data transfers are to be executed "*under the law of the requested Member State*".

VIII Question 5: Access to information on the implementation of the Agreement

76. The fifth question of Mr López Aguilar reads as follows (emphasis in the original):

How can the European Parliament be granted access to all the relevant information, even if of confidential nature, linked to the implementation of the interim agreement (Article 10 Review) also bearing in mind the requirements of Article 218(10) TFEU as regards negotiation and conclusion of agreements?

77. Article 10 of the Agreement provides for a procedure to review the implementation of the Agreement, particularly as regards "*the privacy, protection of personal data, and reciprocity provisions*". The review is carried out "*at the request of one of the Parties and in any case after a period of six (6) months*", though Parliament is not expressly included in the process. The Treasury Department must "*ensure access to relevant documentation, systems, and personnel, as well as precise data relating to the number of financial payment messages accessed and the number of occasions on which leads have been shared*". The arrangements by which Parliament could have access to this information is an internal European Union matter which it would not be appropriate to specify in the text of the Agreement, though there is nothing in the Treaties which would prevent the Council laying down such arrangements in the text of the Decision by which the Agreement is concluded.
78. It should be noted that the requirement under Article 218(10) TFEU that Parliament be informed "*at all stages of the procedure*" only refers to the procedure for the adoption of the Agreement. That said, it is clear that the review of the implementation of the Agreement of 30 November 2009 is directly relevant for the negotiation and conclusion of the long-term agreement which is to succeed it, in accordance with Article 15(4). For this reason, and because of its legislative responsibilities under the substantive legal basis on which the Decision concluding the Agreement is to be founded, Parliament is entitled to be kept fully informed of the review.

(signed)

Kieran BRADLEY

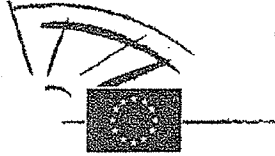
(signed)

Antonio CAIOLA

(signed)

Visa: Ezio PERILLO, Director

Annex: Letter of Mr López Aguilar of 1 February 2010



ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA ĦEORPA PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROOPARLAMENTET

IPOL-COM-LIBE D (2010) 5004

301299 01.02.2010

Mr Christian PENNERA
Jurisconsult
KAD 06 A 007
LUXEMBOURG

Dear Jurisconsult,

Having regard to 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 (EU-US TFTP) as signed on 30 November 2009¹ and bearing in mind the issues already raised by the European Parliament, notably in its resolution of 17 September 2009²,

I would be grateful if you could advise the Committee on Civil Liberties, Justice and Home Affairs (LIBE) on the following legal issues:

- 1. Should the legal basis of the proposal for a Council Decision on the conclusion of the above-mentioned agreement also refer explicitly to Article 16 TFEU (data protection) and the now binding Charter of Fundamental Rights?*
- 2. Should the European Parliament refuse to give its consent, under what conditions and safeguards could the US obtain information covered by this EU-US agreement from the Member States?*
- 3. To what extent are the provisions of the EU-US TFTP interim agreement in line with the European Parliament resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing, notably paragraphs 2, 7, 8 and 11?*

¹ [2010] OJ L 8/11.

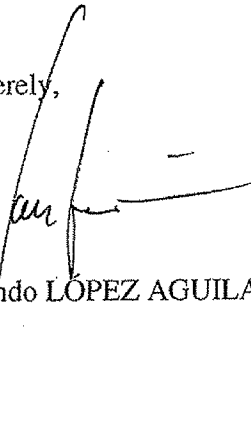
² European Parliament resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing (P7_TA-PROV(2009)0016).

4. What is the exact meaning of Article 13 which underlines that ' the Agreement is not intended to derogate from or amend the laws of the United States or the European Union or its Member States'? Should it be understood then that the final rule applicable as regards the transfer of data is the national legislation of the requested Member State?

5. How can the European Parliament be granted access to all the relevant information, even if of confidential nature, linked to the implementation of the interim agreement (Article 10 Review) also bearing in mind the requirements of Article 218(10) TFEU as regards negotiation and conclusion of agreements?

I would be grateful if you could also comment on any other aspect that you consider relevant.

Yours sincerely,



Juan Fernando LÓPEZ AGUILAR

cc. Mr Klaus Welle, Secretary-General of the European Parliament
Mr David Harley, Deputy Secretary-General Director General
Mr Riccardo Ribera d'Alcala, Directorate-General for Internal Policies

cc: LIBE VPs :Ms Kinga Gál
Ms Sophia in 't Veld
Mr Salvatore Iacolino
Ms Kinga Göncz

Coordinators : Mr Simon Busuttil
Ms Jeanine Hennis-Plasschaert
Mr Raül Romeva i Rueda
Mr Timothy Kirkhope
Mr Rui Tavares
Mr Claude Moraes
Mario Borghezio