Council of the
European Union

Brussels, 16 February 2015
(OR. en)

11897/09
DCL 1

JUR 320
JAI 465
USA 57
RELEX 652
DATAPROTECT 48
ECOFIN 513

DECLASSIFICATION

of document:	ST 11897/09 RESTREINT UE
dated:	9 July 2009
new status:	Public
Subject:	Recommendation from the Commission to the Council to authorise the opening of negotiations between the European Union and the United States of America for an international agreement to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing (doc. 11009/09 RESTREINT JAI 397 USA 43 RELEX 574 DATAPROTECT 42) - **Legal basis**

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

COUNCIL OF
THE EUROPEAN UNION

Brussels, 9 July 2009
(OR. en)

11897/09

RESTREINT UE

JUR 320
JAI 465
USA 57
RELEX 652
DATAPROTECT 48
ECOFIN 513

OPINION OF THE LEGAL SERVICE *

Subject : Recommendation from the Commission to the Council to authorise the opening of negotiations between the European Union and the United States of America for an international agreement to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing (doc. 11009/09 RESTREINT JAI 397 USA 43 RELEX 574 DATAPROTECT 42)
- Legal basis

I. INTRODUCTION

Both in the course of the discussions held in Coreper on 24 June 2009 and following an intervention of the representative of the Council Legal Service in the Group of JHA Counsellors meeting on 1 July 2009, the Legal Service was requested to formulate its opinion on the legal aspects of the above-mentioned Recommendations in writing. This opinion responds to that request.

1. The explanatory memorandum to the above-mentioned Recommendation from the Commission recalls that the United States Department of the Treasury has developed a Terrorist Finance Tracking Program (TFTP). TFTP is a programme under which the Treasury Department requires, by means of administrative subpoenas [1], the Society for Worldwide Interbank Financial Telecommunications (SWIFT) in the United States to transfer to the Treasury Department sets of financial messaging data transiting over SWIFT's financial messages network and which are stored by SWIFT in a data base located on US territory. Many of these data originate in European Union Member States.

2. SWIFT is a private enterprise, set up under Belgian law, offering worldwide financial messaging services which facilitate international and other money transfers between financial institutions. SWIFT stores all messages exchanged between its clients for a period of 124 days at two operation centres, one within the EU and one in the USA ("mirroring"). The messages contain personal data such as the names and addresses of the payer and the payee. SWIFT and the instructing financial institutions share joint responsibility for processing of the personal data. SWIFT has more than 8500 clients, mostly financial institutions located all over the world, using its services. It processes millions of financial messages per day. In its field of activity SWIFT has a quasi-monopoly position.

3. Following the revelation in June 2006 in US media of the existence of the TFTP and its impact on data processed by SWIFT, the President of the Council of the European Union and the European Commission engaged in 2007 in discussions with the United States Treasury Department concerning the latter's processing of EU-originating personal data accessed under the TFTP. As a consequence of these discussions, the Treasury Department adopted a series of unilateral commitments to the European Union (the TFTP Representations) [2].

---

[1] The US legal bases for these subpoenas are the International Emergency Economic Power Act of 1997 (IEEPA) and Executive Order 13224. The IEEPA is a statute passed in 1977, which allows the United States government to compel the production of information pursuant to a Presidential declaration of national emergency. In the case of SWIFT the subpoenas have been issued pursuant to President Bush's declaration of an emergency with respect to terrorism after September 11th in Executive Order 13224. That declaration has been renewed every year since, in light of the continuing threat posed by Al-Qaeda and other terrorist groups.

[2] OJ C 166 of 20.7.2007, p. 18-25.

4. In view of criticism voiced against the existing arrangement[3], SWIFT announced in 2007 that it would introduce a new system by the end of 2009. According to the new system, the European zone will consist of the current European operating Centre accompanied by a new operating centre based in Switzerland. Intra-European zone messages will only be processed and stored within their zone of origin. The effect of the new system is that a significant part of data which were the object of TFTP subpoenas will no longer be transferred to the United States in order to be stored there [4].

5. As a consequence of the imminent introduction by SWIFT of its new messaging structure, the Commission has presented a recommendation to the Council to authorise the opening of negotiations with the United States regarding an international agreement to require the transfer to the United States of relevant financial messaging data which are necessary for the purpose of the fight against terrorism and its financing. The Agreement would provide a system according to which "a public authority" would be designated in Europe. This "authority" would receive requests from the United States Department of the Treasury for the transfer of financial payment messaging data stored in the operation centre in the EU, so as to allow the American authorities to continue to run the TFTP in the same manner as before the restructuring of SWIFT's messaging architecture. On receipt of such requests, the "authority" would verify the legality of the request according to the Agreement and, as appropriate, order SWIFT to transfer data to the US authorities. According to the Commission, this Agreement, should be negotiated on the basis of Articles 24 and 38 TEU.

[3] In its Opinion 10/2006, the Article 29 Working Party established by Directive 95/46/EC stated that the continued processing of personal data, knowing the large scale of US subpoenas, is a further purpose which is not compatible with the original commercial purpose for which the personal data were collected.
In the same opinion, the Article 29 Working Party also stated that it is always possible to mirror processing outside the EU or EEA in a country that provides an adequate level of protection. The WP referred to countries such as Argentina or Canada which, according to European Commission Decisions, are considered as satisfying the requirements of Directive 95/46/EC. The "mirroring" in a non-EU country without an adequate level of data protection cannot be justified by Article 26 (1) (d) of Directive 95/46/EC.

[4] According to the Belgian Data Protection Commission, the introduction of this new system is an adequate measure to ensure the protection of personal data and it has encouraged SWIFT to adopt it.

II. LEGAL ANALYSIS[5]

6. According to Article 47 TEU, nothing in the TEU shall affect the Treaties establishing the European Communities. Articles 24 and 38 TEU can therefore only constitute bases for the Agreement if the Community does not have any competence to act in the area of the proposed Agreement.

External Community competence

7. Exclusive external Community competence may result from the content of measures in secondary legislation already adopted [6] which satisfies the criteria developed in the AETR case-law. In the AETR case [7], the Court of Justice ruled that, once the Community has exercised its internal competence by adopting provisions laying down common rules, the Community acquires exclusive external competence in the sense that Member States no longer have the right acting individually or even collectively to undertake obligations which would affect or be capable of affecting those rules.

8. According to the Court of Justice [8], any external competence of the Community must have its basis in conclusions drawn from a specific analysis of the relationship between the agreement envisaged and the Community law in force from which it is clear that the conclusion of such an agreement is capable of affecting the Community rules.

However, it is not necessary for the areas covered by the international agreement and the Community legislation to coincide fully. The assessment as to whether an area is already covered to a large extent by Community rules must be based not only on the scope of the rules in question but also on their nature and content. It is also necessary to take into account not only the current state of Community law in the area but also its future development, insofar as that is foreseeable at the time of analysis [9].

---

5 The present opinion is limited to the question of the legal basis and does not address other questions raised by the proposed mandate and negotiating Directives.

6 Even in the absence of internal measures the Community has exclusive competence to conclude an international agreement if it is necessary in order to achieve a Treaty objective which cannot be attained by the adoption of autonomous rules.

7 Case 22/70 Commission v. Council [1971] ECR, 263.

8 Opinion 1/03 of 07.02.2006, para 124.

9 Ibidem, para 126. In the proposed negotiating Directives, the Commission has indicated that in the event of the EU setting up an EU TFTP, competent United States authorities should agree to transfer relevant financial messaging data to competent European Union authorities.

The ECJ has stressed that the existence of an exclusive external competence of the Community in order to preserve the full effectiveness of Community law is essential to ensure not only the uniform and consistent application of the Community rules as such, but also **the proper functioning of the system which they establish** (emphasis added) [10].

The system established by the Community in the fight against terrorist financing

9. In the area relating to the proposed Agreement, the following adopted Community acts are relevant:

A. Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. This Directive is based on Article 47(2) and Article 95 of the TEC.

10. The objective of this Directive is the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (recital 46). It is in line with international standards set out in the Recommendations of the Financial Action Task Force (FATF), especially its Special Recommendations on Terrorist Financing of 2004, the 1999 UN Convention for the Suppression of the Financing of Terrorism (Art. 18(1)(b)) and the 2005 Council of Europe Convention on the laundering, search, seizure and confiscation of proceeds from crime and terrorist financing (Arts. 2 and 13(2)).

11. According to the Directive, the financial institutions and other legal and natural persons covered by the Directive must apply various levels of customer due diligence measures as set out in Chapter II thereof. Moreover, they are to be made subject to reporting obligations under the provisions of Chapter III, requiring them to report individual cases of suspicious financial transactions to financial intelligence units (FIUs) set up in each Member State . And finally, they are to be made subject to the obligation to keep documents and information as referred to in Chapter IV for use in any investigation into an analysis of possible money laundering or terrorist financing.

[10] Opinion 1/03, paras 128, 131 and 133.

B. Regulation (EC) Nº 1781/2006 of 15 November 2006 on information on the payer accompanying transfers of funds.

12. This Regulation is based on Art. 95 TEC and lays down rules on information on the payer which has to accompany transfers of funds for the purposes of the prevention, investigation and detection of money laundering and terrorist financing (Article 1). It seeks to transpose uniformly throughout the Community the Special FATF Recommendation VII.

13. The Regulation applies to transfers of funds, in any currency, which are sent or received by a payment service provider established in the Community. The service providers covered by the Regulation must obtain complete information on the payer, consisting of his name, address and account number, and ensure that transfers of funds are accompanied by complete information on the payer (Article 4 paragraph 5).The payment service providers must keep records for five years of any information received on the payer (Article 11).

14. According to Article 14 of the Regulation, the payment service providers have to respond fully to enquiries from the authorities responsible for combating money laundering and terrorist financing in the country where they are situated.

Would Community rules be affected by the proposed Agreement with the United States?

15. With the above two legislative acts, the Community has set up a more or less complete system of measures defining the role of economic operators, and in particular the financial institutions in the EU, in action to be taken against terrorist financing. This system, following the model of the FATF Recommendations and the UN and Council of Europe Conventions, is the result of a balancing of the need to have effective tools against terrorist financing against the need to respect the privacy interests of the customers of financial operators. According to this system, a particular responsibility lies with the financial institutions and other financial service providers, leaving it up to them to alert the public authorities in cases where they have reasons to believe that certain transactions are suspicious or irregular and are therefore to be reported.
It is on this basis that these institutions and operators and their clients establish their mutual relations.

16. The fact that this system is the result of a balancing of interests has been expressly laid down in the recitals of the acts concerned, which not only state that they respect fundamental rights and observe the principles recognised in the Charter of Fundamental Rights of the EU, but also that, in accordance with the principle of proportionality as set out in Article 5 of the Treaty, they do not go beyond what is necessary in order to achieve their objectives.

17. The present US system for countering terrorist financing, and in particular the TFTP of the US Department of the Treasury, is different from that of the Community, in so far as it does not rely on the initiative of the financial institutions to report their suspicions to the Government, but rather allow for the Government to have data about financial transactions transferred to it in large quantities, irrespective of any particular suspicion, in order to let the Government examine whether its analysis of those data leads it to harbour certain suspicions.

18. It might be argued that SWIFT as such is not directly concerned by the above-mentioned two Community acts, since SWIFT is not itself a financial institution within the meaning of the Directive, it does not generate personal data of its own, and it does not itself have access to the personal data contained in messages transferred through its messaging system and that, therefore, the existing Community rules would not be affected by imposing transfer obligations exclusively on SWIFT.

However, the Legal Service is of the view that such a position would misrepresent the role and function of SWIFT in the entire financial world. As it appears unequivocally from the Decision of 9 December 2008 of the Belgian Data Protection Commission[11], SWIFT cannot be considered in isolation from its clients and users. If SWIFT were subjected to an obligation to transfer in bulk data (on financial transactions between its users) held in its operating centres to governmental authorities in order to be analysed for possible leads to terrorist financing, that would undoubtedly affect the functioning of the Community system, according to which it is up to the clients and users of SWIFT to determine what specific transactions should be reported.

The position of the financial institutions, subject to the Community acts referred to above, both vis-à-vis the national authorities of the Member States of their location and vis-à-vis their customers, would be affected.

[11] Accessible through http://www.privacycommission.be/fr/press_room/pers_bericht11.html.

Relevance of the case-law of the ECJ in the PNR cases

19. In its explanatory memorandum to the Recommendation, the Commission indicates that "the jurisprudence of the Court of Justice provides that direct access to data by law enforcement services engaged in a law enforcement activity cannot be regulated on a Community basis. An international agreement for the transfer to the United States of relevant financial messaging data for the fight against terrorism and its financing should therefore be addressed on the basis of Title VI TEU."

20. The case-law to which the Commission refers is the ruling of the ECJ in Joint Cases C-317/04 and C-318/04 (EC-US PNR Agreement). In these cases, the European Parliament sought the annulment of:

- Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (CBP). This Agreement was based on Articles 95 and 300 TEC; and

- Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States. This Decision was based on Article 25(6) of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data.

21. In its findings in Case C-318/04, the Court of Justice noted that the Commission's Decision on adequacy concerned only PNR data transferred to CBP. In the view of the Court, that transfer constituted processing operations concerning public security and activities of the State in areas of criminal law which are excluded from the scope of Directive 95/46/EC according to Article 3(2) thereof. It consequently annulled the Decision on adequacy .

22. In its findings in Case C-317/04, the Court of Justice ruled that Article 95 EC **read in conjunction with Article 25 of Directive 95/46/EC** (emphasis added), cannot justify Community competence to conclude the Agreement. The Agreement related to the same transfer of data as the Decision on adequacy and therefore to data processing operations which are excluded from the scope of the Directive. It consequently annulled the Council Decision.

23. Indeed, the PNR-Agreement relied entirely on the powers exercised by the Community through the adoption of Directive 95/46/EC[12] and the adoption of an adequacy Decision by the Commission pursuant to that Directive[13] .
Having annulled the Commission's adequacy Decision, the Court could not come to any other conclusion than it did in respect of the PNR-Agreement itself and the Council Decision pertaining to its conclusion.

24. However, it must be observed that the Court did **not** state in its judgement what the appropriate legal base should be for concluding the Agreement with the US. In particular, it did not state that the conclusion of the Agreement falls within the powers of the Union as a matter falling under Title VI TEU. It restricted itself to finding that Directive 95/46/EC, in Article 3(2), first indent, and as confirmed in its 13th recital, does not apply to the processing of personal data "*in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI TEU*". In the terms of recital 13, "*the activities referred to in Titles V and VI TEU regarding public safety, defence, State security or the activities of the State in the area of criminal law fall outside the scope of Community law, **without prejudice to the obligations incumbent upon Member States under Article 56(2), Article 57 or Article 100a TEC***" (emphasis added).

---

[12] 3rd recital: *"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, and in particular Article 7(c) thereof".*

[13] 5th recital: "*Having regard to Commission Decision C(2004) 1799 adopted on 17 May 2004 pursuant to Article 25(6) of Directive 95/46/EC […](hereinafter "the Decision")*" and point 2 of the Agreement: *"Air carriers operating passenger flights in foreign air transportation to or from the US shall process PNR data contained in their automated reservation systems as required by CBP pursuant to US law **and strictly in accordance with the Decision for so long as the Decision is applicable."*** (emphasis added).

25. It is clear that, by making reference to activities referred to in Titles V and VI TEU, the Community legislature intended to describe the sort of situations that it wished to exclude from the scope of the Directive. However, it cannot be inferred from these provisions that:
a) there would be no possibility under Article 95 TEC to enlarge the scope of Directive 95/46/EC beyond its present field of application[14] ; and
b) that it would be possible under Title VI TEU to adopt legal instruments obliging economic operators to retain data, collected in the exercise of their commercial activities, in order to allow for law enforcement authorities to have access to those data, or to regulate the way in which economic operators should make such data available for law-enforcement purposes[15].

26. There is an important difference between the "PNR situation" as it existed in 2006 and the "SWIFT situation" of today. The difference is that in 2006 there did not exist any internal Community legislation obliging air transport service providers to report data about their customers to the authorities with a view to contributing to the fight against terrorism and other serious forms of crime, which was the objective for which PNR data were to be transferred to the US administration. For financial institutions, however, the Community has already exercised its competence and adopted in 2005 and 2006 legislation introducing obligations, as referred to in paragraphs 9 and 12 of this opinion, which have the very purpose of helping to counter terrorist financing, including the obligation to report suspicious transactions to national authorities to be used for law enforcement purposes.

[redacted]

[14] See the Contribution of the Legal Service in Doc. 16614/07 of 18 December 2007 JUR 462 CRIMORG 194 AVIATION 229 DATAPROTECT 61, paragraphs 20 and 30, point b).
[15] See the Contribution of the Legal Service referred to in the previous footnote, paragraph 17.

Implications of having existing internal legislation affected

27. As indicated in paragraph 18 of this opinion, the functioning of the system set up by these Community acts would clearly be affected by the conclusion of an agreement as recommended by the Commission. Following the well-settled case-law of the Court of Justice, the existence of Community legislation entails an exclusive competence for the Community to negotiate and conclude any international agreement that would affect or be capable of affecting that legislation. Therefore, there is also in this case an exclusive competence for the Community to negotiate and conclude such an agreement affecting the Directive and Regulation in question and the proper functioning of the system which they establish. The legal basis on which the Community is to exercise its external competences must be the same as the one on which it exercised its internal powers, that is to say Article 95 TEC. Therefore, the signature and conclusion of the suggested Agreement on the basis of Articles 24 and 38 TEU would amount to a violation of Article 47 TEU.

28. The Legal Service does not see any obstacle to using Article 95 TEC as the basis for the conclusion of the recommended Agreement with the US. Indeed that provision, which could not be used as the basis for the PNR Agreement with the US, given its reliance on Directive 95/46/EC based on that Article, offers scope for the adoption of other Community legislation than merely in the area of processing of personal data and the free movement of such data. The acts adopted by the Community on the basis of Article 95 TEC for the specific purpose of involving financial institutions in the fight against money laundering and terrorist financing demonstrate this. Moreover, even though Directive 95/46/EC, including its Article 25(6), does not apply to the transfer of data under the recommended agreement, this fact would not preclude the Community from negotiating with the US such commitments from the US side with regard to the treatment and protection of transferred personal data as would satisfy an adequate level of compliance with data protection principles upheld by the Community.

Elements of the negotiating directives which fall, or might fall, outside the competence of the Community

29. It is true that certain elements of the proposed negotiating directives, considered in isolation, are (possibly) falling outside the powers of the Community.

30. For instance, the assurance that the competent US authorities will make available information extracted from the TFTP data base to the competent authorities of one or another Member State (assuming that the latter are authorities as referred to in Article 29 TEU), to Europol and Eurojust would, if deemed necessary, require another legal basis. At first glance, that element seems already to be covered by existing Agreements between the US and the EU (on Mutual Legal Assistance in Criminal Matters, Art. 4, based on Arts. 24 and 38 TEU)), or Europol (Art. 4(4)) or Eurojust (Art. 8(2)) (based on the respective constituting acts of Europol and Eurojust). If further analysis would confirm that such is the case, this element could be omitted from the negotiating directives. Otherwise, it might be considered to have the existing Agreements adjusted in conformity with the procedures applicable to their modification.

31. As far as the "authority", referred to in paragraph 5 of this opinion, is concerned, the description of this "authority" given so far by the Commission is very vague. In the absence of more concrete information as to what is actually envisaged, it is not possible for the Legal Service to take a position as to the legal basis on which such an "authority" could be established or designated, taking into account in particular the nature of the powers with which such an "authority" would be vested and the way in which such powers were to be enforced.

III. CONCLUSION

32. The Council Legal Service is of the opinion that Council Directive 2005/60/EC of 26 October 2005 and Regulation (EC) Nº 1781/2006 of 15 November 2006 and the functioning of the system which they establish of involvement of financial institutions in action against terrorist financing would be affected by an Agreement with the United States as envisaged. Consequently, it is for the Community to negotiate and conclude such an Agreement on the basis of Articles 95 and 300 TEC.