



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 23 October 2009

**11897/09
EXT 1**

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

PARTIAL DECLASSIFICATION

of document: 11897/09 RESTREINT UE

dated: 9 July 2009

new classification: none

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 partially declassified version of the above-mentioned document.



ANNEX

**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 9 July 2009

**11897/09
EXT 1 (23.10.2009)**

**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.

*

"This document contains legal advice protected under Article 4(2) of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, and not released by the Council of the European Union to the public. The Council reserves all its rights in law as regards any unauthorised publication."

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 arrangement³, 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 there⁴.

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. **NOT DECLASSIFIED**

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.

NOT DECLASSIFIED FROM THIS POINT UNTIL THE END OF THE DOCUMENT

(page 12)
