EDPS Comments on the Recommendation from the Commission to the Council to authorise 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

I. Introduction

The EDPS was consulted by the European Commission on 18 June 2009 about its Recommendation to Council for the negotiation of an international agreement to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing.

The Commission recommendation, as explained in its explanatory memorandum, was triggered by the changes in the architecture of SWIFT, which by the end of 2009 will ensure that SWIFT financial transaction messages which are internal to the European Economic Area and Switzerland will remain within the European zone - as different from the transatlantic zone - and will no longer be mirrored in the US operating centre. This change in the architecture was encouraged and welcomed by EU data protection authorities[1], as it was designed to bring all EU-originating data within the control of EU authorities and thus ensure that the EU standard for the protection of fundamental rights, including the protection of personal data, would fully apply.

With the current recommendation the Commission envisages an international agreement between the EU and the US, which, based on Article 24 and 38 TEU - i.e. a third pillar legal basis -, would require transfer to the United States Department of Treasury of relevant financial messaging data which are necessary for the purpose of the U.S. Treasury Department's Terrorist Finance Tracking Programme.

[1] - Opinion of the Article 29 Working Party of 22 November 2006, WP 128.
- EDPS opinion of 1 February 2007. In this opinion the EDPS noted that "*[i]t is also a matter of sovereignty to prevent that data relating to citizens and companies based in the EU are accessed by third countries authorities without respecting the conditions and safeguards that would be imposed to similar authorities within the EU*".

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

The new SWIFT architecture will consist of two processing zones, a European and a transatlantic zone. Since inter-zone traffic will be stored, both at the sending and the receiving end, the current change in SWIFT architecture will not reduce the U.S. Treasury capacity to access data concerning payments between the EU and the US. Instead, the Commission proposal targets personal data related to financial transactions which have no specific connection with the United States, but relate mainly to intra-European payments as well as to payments between the EU and third countries, and between third countries (for those third countries opting to have their traffic stored in the European zone). With regard to intra-European payments, it shall be noted that the creation of the Single European Payment Area (SEPA) has considerably increased the number of transactions carried out in the EU through the SWIFT network, which now is used also for transactions with a non cross-border nature.

Therefore, the recommendation envisages an agreement whereby information relating to EEA - as well as third countries - financial transactions which are stored in EU territory will be made available to U.S. authorities upon administrative orders (subpoenas) issued by U.S. Treasury Department officials.

II. Necessity and proportionality of a possible agreement

The EDPS has considered with great attention the initiative of the Commission aiming at an agreement with the United States to make financial messaging data stored in the EU available to US authorities.

The EDPS considers such proposal as very privacy-intrusive, as it foresees important derogations to the European data protection framework and a limitation of the sovereignty of the EU.

The EDPS considers that there must be very strong evidence that such an intrusive measure is needed. If this evidence is given, it must be ensured that rights of European citizens are fully safeguarded.

The EDPS notes that the EU has developed in recent years a European approach against terrorism financing. He refers in particular to Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds.

Both instruments contain a number of measures aimed at combating the misuse of the financial system for the purpose of money laundering and terrorist financing. They also contain specific provisions allowing exchange of information with third countries authorities as well as safeguards for the protection of personal data, in line with Directive 95/46/EC. In particular, Regulation 1781/2006 takes specifically into account the developments in the international context, by implementing the Special recommendations against Terrorist Financing adopted by the Financial Action Task Force (see Recital 3).

Furthermore, the agreement on mutual legal assistance between the EU and the US (6 June 2003) explicitly allows the exchange between law enforcement authorities of information relating to bank accounts and financial transactions, providing conditions and limitations with regard to this exchange. In addition, instruments for the exchange of data between the US and Europol and Eurojust are already in place, ensuring at the same time exchange of information and protection of personal data.

Pursuant to Article 8 ECHR, a public authority may interfere with the exercise of the right to private life only when this is necessary in a democratic society to pursue one of the listed public interests. This provision is not only binding for all the Member States, but according to Article 6(2) TEU also for the Union itself. This is confirmed by the EU Charter of Fundamental Rights, which will be binding as soon as the Treaty of Lisbon is ratified and enters into force.

Against this background, the need for a specific international agreement in this area with the U.S. is not self-evident and the Commission recommendation fails to explain and provide evidence that existing EU instruments and international agreements cannot be satisfactorily used and that such a privacy-intrusive instrument is needed.

The EDPS is also concerned about the influence of the envisaged system of collection of data on the present EU framework, and the risk of lowering the level of data protection within the EU. Particular attention shall be paid to the conditions of use of the TFTP programme by European law enforcement authorities, and the possible setting up within the EU of an equivalent programme.

Besides, the EDPS has serious doubts about the general lawfulness of the whole scheme, considering that the draft mandate already foresees possibilities of claims originating from third countries and a related compensation from the US to the EU in relation to these claims. The EDPS questions whether an international agreement can validly identify - and to some extent acknowledge - shortcomings and legal claims against its implementation, without

putting into question the lawful character of the measures which will lead to such expected claims.

The EDPS notes finally that this initiative is taken before the Lisbon Treaty enters into force and that after Lisbon also the adoption of third pillar agreements would need the approval of the European Parliament. Instead, the timing of the current proposal would entail that the Parliament will play a more limited role and that there will only be very little room for political debate on the proposal. The EDPS believes that decisions on a possibility for such a large-scale access by third countries to EU data need a careful assessment and a public debate with full involvement of the European Parliament.

III. The legal basis

The legal basis of the agreement between the EU and the US would be, according to the proposal, Articles 24 and 38 of the Treaty on European Union. It is thus a third pillar instrument, with consequences mentioned above in terms of absence of democratic control. The EDPS is not convinced by the validity of this legal basis and asks Commission and Council to reconsider it.

The explanatory memorandum of the proposal justifies the legal basis by the fact that "direct access to data by law enforcement services engaged in law enforcement activity cannot be regulated on a Community basis".

This leads to several questions.

As mentioned above, EU legal instruments aiming at fighting money laundering and terrorist financing are based on a Community basis, notably Article 95 TEC. Just as the international agreement envisaged by the Commission, these Community legal instruments specifically impose obligations on private parties and deal with exchanges of data between competent authorities responsible for combating money laundering and terrorist financing, also in case these authorities operate in third countries.

The similarity of these Community instruments with the TFTP is also explicitly highlighted by the TFTP Representations, which in the Chapter relating to International Counterterrorist Financing Principles, state that *"[i]n Europe, similar provisions have been implemented into national law consistent with the Third Money Laundering Directive and, most recently, Regulation (EC) No 1781/2006* [...]".

Against this background, the EDPS notes that, pursuant to well-established case law of the Court of Justice, recently confirmed by its judgement on the data retention Directive, "*under Article 47 EU, none of the provisions of the EC Treaty may be affected by a provision of the EU Treaty*" and therefore measures coming within the scope of Community powers could not be based on a provision of the EU Treaty without infringing Article 47 thereof.

Therefore, the EDPS notes that there are reasons to consider that both the envisaged international agreement and a possible future EU TFTP come within Community powers and should therefore be based on first pillar provisions.

In any case, even if these legal instruments had to be considered outside the scope of Community law, EU competence under the third pillar would not be automatic. Indeed, the connection with police and judicial cooperation between EU authorities is only indirect and to a large extent merely prospective, stemming only from the obligation on US authorities to feed data back to EU authorities.

It should also be noted that in the similar area of restrictive measures on suspected terrorists, EU action and international cooperation have so far been based on the Common Foreign and Security Policy ("second pillar").

IV. Applicable standards and safeguards for the protection of personal data

The EDPS agrees with the part of the explanatory memorandum stating that appropriate safeguards are necessary for the transmission of relevant data to the US authorities and that such safeguards must ensure full respect for fundamental rights enshrined in Article 6(2) TEU and for the principle of proportionality and necessity regarding the right to respect for private and family life as set out in Article 8(2) ECHR. According to the EDPS, account should also be taken of Council of Europe Convention 108 and its additional Protocol, as well as of Article 8 of the EU Charter of Fundamental Rights, which is applicable to all areas of EU activity and spells out the basic elements of the right to the protection of personal data.

Indeed - and as opposed to the PNR agreement - in this case there is no element of connection between the data being processed and the US: the controller is established in the EU, the database is in the EU, and the data processed relate to any kind of financial transaction worldwide.

However, the negotiating directives refer to a different data protection standard, stating that "*Safeguards and controls regarding the protection of personal data transferred to the United States Department of Treasury pursuant to the Agreement, including the monitoring of such safeguards and controls, shall be at least equivalent to those set out in the TFTP Representations*".

With regard to this point, the EDPS notes that TFTP Representations are unilateral commitments taken by U.S. authorities with regard to the processing of personal data stored in US territory and thus subject to US jurisdiction. These representations do not include all elements required by EU standards of protection of fundamental rights - and in particular data protection -, that become fully applicable when data are stored on EU territory.

With regard to the applicable data protection standards, the EDPS recommends that, would the necessity of an agreement be clearly established, *quod non*, the negotiating guidelines request that data protection safeguards in the envisaged agreement refer to the standards laid down by Article 8 of the EU Charter of Fundamental Rights and to Council of Europe Convention 108 rather than to the standards set by the TFTP representations.

In this perspective, the negotiating guidelines should also explicitly single out those data protection safeguards that are essential conditions for an agreement with the US. In particular, the EDPS recommends that a possible agreement shall ensure that:

- Data are only transferred and processed to fight terrorism, the definition of terrorism being the one laid down by Article 1 of the Council Framework Decision 2002/475/JHA on Combating Terrorism.
- Data are transferred through a "push" rather than a "pull" system[2]. SWIFT shall keep a record of every transfer of personal data taking place on the basis of the agreement. This record shall be put at the disposal of competent data protection authorities upon request.
- US requests are subject to the same conditions and safeguards, including possible judicial authorisation, as requests of European law enforcement authorities.
- Searches on SWIFT databases are proportionate, narrowly targeted and based on suspicions concerning specific persons. With regard to the storage period, the international agreement shall ensure that personal data are kept for no longer than necessary for the specific investigation for which they were collected.

[2] In that sense the system mentioned in the draft mandate, including the intermediary role of a public authority, might contribute to comply with data protection requirements, depending on details of implementation.

- Further sharing of personal data by the US Treasury with other national authorities shall be limited and sharing with other countries or international organisations shall be subject to the same conditions as those laid down for EU law enforcement authorities pursuant to applicable data protection legislation, in particular Convention 108 and, where relevant, Article 13 of the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

- In the course of the reviews carried out by the EU, the US Treasury shall be required to justify not only the geographical scope of requested financial messages, but shall also provide precise data concerning the quantity of financial messages processed and the extent to which these data have been shared with other US agencies and/or third countries or international organisations.

- The supervisory competence and powers of EU data protection authorities competent for the supervision of data processing by SWIFT, by financial institutions and by EU law enforcement authorities are in no way limited by the international agreement. Independent supervision, which is one of the essential elements of the EU data protection regime, will include *inter alia* the power to keep supervising how these EU-established controllers comply with applicable data protection law and ensure data subjects' rights, notably the rights to access and rectification. Enforcement powers may also include the power to hear complaints and to order the blocking of the transfer of relevant financial messaging data.

- Redress mechanisms are available as well as compensation in case of unlawful processing of personal data. This is a particularly important issue especially in those cases where data extracted from EU territory are used in order to designate individuals - including EU citizens - as terrorists and freeze their assets or in order to impose economic sanctions also on EU companies[3].

- The agreement does not result in circumventing EU conditions and safeguards laid down for the processing of personal data by EU competent authorities, including Europol and Eurojust.

V. Conclusions

[3] In some cases, even if actions taken by these companies do not constitute a breach of national or EU laws. See TSB Lloyds case at http://www.politics.co.uk/news/foreign-policy/govt-dismisses-lloyds-tsb-sanction-concerns-$1268756.htm.

The EDPS recommends the Commission and the Council to:

- Reconsider the necessity and proportionality of an agreement, particularly in consideration of the privacy-intrusiveness of the proposal and of the existence of a well-developed EU and international legal framework in this area.
- Reconsider the proposed legal basis.
- In any case, would the necessity of an agreement be clearly established, amend the negotiating guidelines as suggested in Chapter IV, in particular by explicitly laying down the data protection standards and safeguards that are essential conditions for the respect of the EU fundamental right to the protection of personal data, and thus for the conclusion of an international agreement.

Brussels, 3 July 2009