19.2.2010

NOTICE TO MEMBERS

Subject: **Petition 1097/2009 by Alexander Junger (Austrian), on the proposed exchange of banking data between the EU and the United States, on the pretext of combating terrorism**

1. Summary of petition

The petitioner considers the proposal of revealing banking data to the authorities of the US - on the pretext of combating terrorism - as an infringement of banking secrecy and of the personal integrity of European citizens.

2. Admissibility

Declared admissible on 19 November 2009. Information requested from Commission under Rule 202(6).

3. **Commission reply**, received on 19 February 2010.

The petitioner claims that revealing banking data to the US authorities constitutes an infringement of banking secrecy. He doubts the value of the US Terrorist Finance Tracking Programme (TFTP) and criticises the preventive suspicion of everyone.

The TFTP has existed for eight years. It was set up by the United States Department of the Treasury shortly after the terrorist attacks of 11 September 2001. The TFTP is based on U.S. statutory authorities, UN Security Council Resolutions and related executive orders. A series of press articles in 2006 revealed the existence of the TFTP and led to criticism that the TFTP did not take account of EU data protection law. To address these concerns, the German Presidency of the Council of the European Union (first semester 2007) supported by the Commission, negotiated a set of undertakings with the U.S. Treasury Department concerning

how EU-originating personal data would be processed under the TFTP. These undertakings were published in the Official Journal of the European Union in July 2007 [C 166/18 of 20.7.2007] and include, for example, a strict counter-terrorism purpose limitation, a prohibition on data mining and obligations to delete data within specified timeframes. Additionally, SWIFT US branch joined to Safe Harbour programme which certifies an adequate level of data protection and allows transferring of personal data from the Community to US for commercial purposes.

An assessment of the value of the TFTP for EU security and implementation of US undertakings was made by the French counter terrorism judge Mr. Jean-Louis Bruguière in his report to the European Commission of December 2008. The Report concluded that the TFTP has been of considerable value to EU Member States in their fight against terrorism. More than 1450 TFTP-generated leads have been passed to date to European governments and 800 have been passed to non-European governments, with over 100 new TFTP-generated leads provided to EU countries from January to September 2009. Concrete examples of the benefits of TFTP-derived information include:

(i) TFTP information provided substantial assistance to European governments during investigations into the Al-Qa'ida-directed plot to attack transatlantic airline flights travelling between the EU and the United States. TFTP information provided new leads, corroborated identities and revealed relationships among individuals responsible for this terrorist plot. In mid-September 2009 three individuals were convicted in the UK, and each was sentenced to at least 30 years in prison;

(ii) In early 2009 TFTP-derived information was used to identify financial activity of a Europe-based Al-Qa'ida individual who played a role in the planning of an alleged attack on aircraft. The information was passed to the governments of European and Middle Eastern countries;

(iii) In summer 2007 the TFTP was used to identify financial activities of members of the Islamic Jihad Union (IJU) in Germany. This information contributed to the investigation and eventual arrest of IJU members plotting to attack sites in Germany. The TFTP continued to provide additional useful information to German authorities following the arrests. The persons subsequently confessed.

The value of the TFTP was accepted by all Member States when they unanimously adopted the Council Mandate for negotiation of the EU-US Agreement. In early 2010 Judge Bruguière will produce a second report which will further address the value of information derived from the TFTP for EU security.

At the end of 2009, SWIFT implemented its new "systems architecture". For this purpose SWIFT has retained its existing EU-based and U.S. servers and has brought into operation a new operating centre in Switzerland. The net effect of this new arrangement is that a significant volume of the data which have in the past been received by the U.S. Treasury Department under the TFTP are no longer stored in and no longer under the jurisdiction of the United States Government. Consequently, the financial payment messaging and related data are stored in the territory of the European Union and can be made available only upon request by the US Treasury Department.

In order to ensure that the TFTP continues to produce the above-mentioned EU and wider global security benefits, it was necessary to put in place an international agreement that allows relevant financial messaging data to continue to be made available to the U.S. Treasury Department. Accordingly in July of this year the 27 Member States in Council unanimously adopted a mandate and negotiating guidelines for an EU-US Agreement for the transfer of financial messaging data for purposes of the TFTP. The EU negotiating team was led by the Swedish Presidency assisted by the European Commission.

In September 2009 the European Parliament issued its Resolution on an envisaged EU-US Agreement for the transfer of financial messaging data for the purpose of the TFTP. The Resolution specifies that the agreement must be for a short duration, that processing of financial messaging data must be strictly for counter-terrorism purposes and that requests for data must be based on specific targeted cases and subject to judicial authorisation.

Following several rounds of negotiations, the Council adopted on 30 November a Decision on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme ("Interim Agreement"). Before the Interim Agreement can be concluded, the European Parliament would have had to give its consent - which it refused in the February 2010 plenary. The Agreement provided for provisional application as from 1 February 2010 (the date on which the EU-US MLA Agreement enters into force) and a maximum duration of 9 months. It would therefore have expired and ceased to have effect on 31 October 2010 or earlier. The Commission intended to propose a new mandate in early 2010 for a subsequent agreement based on the Lisbon Treaty with even greater safeguards on data protection and an even greater involvement of the European Parliament. In the meantime, an interim agreement would have been needed to ensure that there is no lapse in TFTP coverage that will now deprive the EU of important information related to terrorist attacks or investigations.

The Interim Agreement contained significant safeguards for the protection of personal data transferred under the Agreement. These included, for example, a strict prohibition on using the data for any purpose other than the prevention, investigation, detection or prosecution of terrorism or its financing, a strict prohibition on any form of data mining and an obligation to provide effective remedies. The Interim Agreement required the Treasury Department to identify data which were no longer needed for counter-terrorism purposes and to delete them. In other cases, data held on the TFTP database had to generally be deleted within five years from receipt. The Interim Agreement imposed strict obligations on data security and on the persons entitled to access TFTP data.

One of the most significant safeguards was that before TFTP data could have been made available to US, the US Treasury Department should have issued a request based on an ongoing investigation concerning specific conduct relating to terrorism crimes had been committed or where there was, based on pre-existing information or evidence, a reason to believe that it could have been committed. In the absence of such well substantiated request, no data could have been made available to US. This obligation would have been subject to verification by the judicial authority of the requested Member State and external audit, and highlights that the TFTP can only be used where there is a demonstrable and reasonable

suspicion that an identified person is engaged in terrorism or its financing.

The easing of banking secrecy is accepted as a necessary and proportionate measure for the fight against serious crime including the financing of terrorism. This is demonstrated, for example, by 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 and Regulation (EC) No. 1781/2006 of 15 November 2006 on information on the payer accompanying transfers of funds. The EU-US Agreement on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the TFTP includes considerable safeguards on access to financial messaging data which underlines the proportionate approach taken by the Interim Agreement.

Conclusion

The Interim Agreement sought to strike the appropriate balance between measures necessary to ensure EU security on the one hand and the protection of personal data on the other. The Agreement would have been for a short duration, would have prohibited any use of financial messaging data for purposes other than the fight against terrorism, and made clear that requests for data must be based on specific targeted cases and that these are subject to judicial authorisation. Above all, TFTP data would not have been subject to open-ended searching and could only have been used if a direct link with terrorism crimes or its financing had been demonstrated. The proportionality of the Interim Agreement, including compliance with the data protection commitments and an assessment of the on-going value of the TFTP for EU security would have been the subject of a detailed EU review to be undertaken in 2010 by, inter alia, representatives of Member States' Data Protection Authorities.

The TFTP is necessary for European security. The security gap, created by the rejection of the interim agreement needs to be filled. The transfer of data could also be agreed upon bilaterally since data is physically located in one Member State only. Nevertheless, it originates in all EU Member States which is why only an EU solution is tenable. The Commission will therefore come up with a new mandate for an EU-US cooperation on the sustainability of the TFTP.