

**US and EU agreement on exchanging personal data for the purposes of the Terrorist Finance Tracking Program (the TFTP Agreement<sup>1</sup>) – first inspection performed by the Europol Joint Supervisory Body (JSB) raises serious concerns about compliance with data protection principles**

Brussels, 2 March, 2011

**EUROPOL's Joint Supervisory Body recently performed its first inspection at Europol regarding the TFTP Agreement, which entered into force in August 2010. The TFTP Agreement gave the JSB a new task - to monitor whether the Europol respects the provisions of personal data protection principles in the TFTP Agreement when deciding on the admissibility of the US' requests to SWIFT. Europol is tasked with verifying whether the US' requests are proportionate and necessary - according to conditions laid down in the TFTP Agreement. Europol can therefore approve or deny the transfer of SWIFT data to the US.**

**The TFTP Agreement was adopted following the so-called 'SWIFT<sup>2</sup> affair' when it became publicly known that all SWIFT data transfers were stored in a mirror database in the US and that US authorities subjected SWIFT, through legal channels, to hand over the requested financial data (so-called subpoenas). Negotiations between the Belgian Data Protection Authority, EU and US authorities led to a decision made by SWIFT to move the mirroring of European transfers to Europe. Negotiations were then held between EU and US authorities to find a legal solution for the exchange of personal data for the purposes of terrorist finance tracking. The TFTP Agreement is the result of those negotiations.**

Under Article 34(1)<sup>3</sup> of the Europol Council Decision, the JSB is tasked with reviewing Europol's activities in order to ensure that individuals' rights are not violated by the storage, processing or use of data held by Europol.

---

<sup>1</sup> 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 the purposes of the Terrorist Finance Tracking Program, OJ L. 195/5.

<sup>2</sup> Society for Worldwide Interbank Financial Telecommunication.

<sup>3</sup> Article 34(1) states, 'An independent Joint Supervisory Body shall be set up to review, in accordance with this Decision, the activities of Europol in order to ensure that the rights of the individual are not violated by the storage, processing and use of the data held by Europol'.

At its meeting of 11 October 2010, the JSB mandated a team to inspect Europol's implementation of the TFTP Agreement, including all related items. The inspection took place in November 2010.

The inspection team found that some data protection requirements were not being met. The most important finding of the inspection was that the written requests Europol received were not specific enough to allow it to decide whether to approve or deny them. It was found that the US requests were too general and too abstract to allow proper evaluation of the necessity of the requested data transfers. Despite this, Europol approved each request it received. One of the JSB's recommendations is, therefore, that Europol should contact the US Treasury Department to ensure that all future requests for SWIFT data comply with the criteria set out in the TFTP Agreement. The JSB concluded that proper verification of whether the requests are in line with the TFTP Agreement – on the basis of the available documentation – is impossible.

Europol advised that orally-provided information plays a role in its verification of each request. This information is provided to certain Europol officials with the stipulation that no record is made. This kind of procedure prevents JSB from checking whether Europol could have rightly come to its decisions. The JSB was therefore unable to evaluate whether the amount of data transferred to the US from SWIFT was proportionate and necessary, as required by the TFTP Agreement. The significant involvement of oral information renders proper internal and external audit, by Europol's Data Protection Office and the JSB respectively, impossible.

Further information, and the complete list of recommendations given to Europol, can be found in the public version of the JSB's report, available now on its [website](http://europoljsb.consilium.europa.eu/about.aspx)<sup>4</sup>. Due to Europol's classification of the information which was inspected (EU SECRET) the JSB is unable to make the complete report publicly available.

EUROPOL JSB

President Isabel Cruz

---

<sup>4</sup> <http://europoljsb.consilium.europa.eu/about.aspx>