The Hague, 8 April 2011
File no. 2566-566

Europol Activities in Relation to the TFTP Agreement
Information Note to the European Parliament
1 August 2010 – 1 April 2011

Table of contents

1. Introduction

This information note provides the European Parliament (EP) with an overview of Europol's activities under Articles 4, 9 and 10 of the Terrorist Finance Tracking Programme (TFTP) Agreement for the period 1 August 2010 – 1 April 2011. It is produced for information purposes only, with the aim of improving Parliament's understanding of Europol's activities in implementing relevant provisions of the TFTP Agreement. It should be read in the context of the EU Review Report on the Implementation of the TFTP Agreement, which is the definitive report on the implementation of the Agreement, as established by the provisions foreseen in Article 13 of the Agreement.

By way of background Europol has provided earlier briefings on its activities in relation to the Agreement, including to the:

- Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) of the European Parliament on 31 January 2011;
- Standing Committee on Internal Security (COSI) and Article 36 (CATS) meetings held in February 2011; and the
- Europol Management Board (MB) at several meetings, most recently on 23-24 March 2011.

Additionally, Europol submitted comments on the Joint Supervisory Body (JSB) Inspection Report concerning the implementation of the Agreement, which was published on 4 March 2011 and discussed at the LIBE Committee on 16 March 2011. Similarly Europol provided input to the EU review team in support of work to produce the EU Review Report, the results of which were presented by the European Commission to the LIBE Committee on 17 March 2011.

2. Europol's role under the TFTP Agreement

2.1. Summary

The EU-US TFTP Agreement, negotiated by the European Commission and approved by the Council of the EU with the consent of the EP, regulates the transfer of bulk data from the Designated Provider in Europe to US authorities (US Department of the Treasury) in order to support the prevention, investigation, detection, or prosecution of terrorism or terrorist financing.

The Agreement:

- Assigns a verification function to Europol (under Article 4);
- Enables the US Department of the Treasury to spontaneously provide to Europol and other authorities in the EU the results of their processing of the data (under Article 9); and
- Enables Europol and other authorities in the EU to request searches of the data (under Article 10).

2.2. Europol's role under Article 4 of the TFTP Agreement

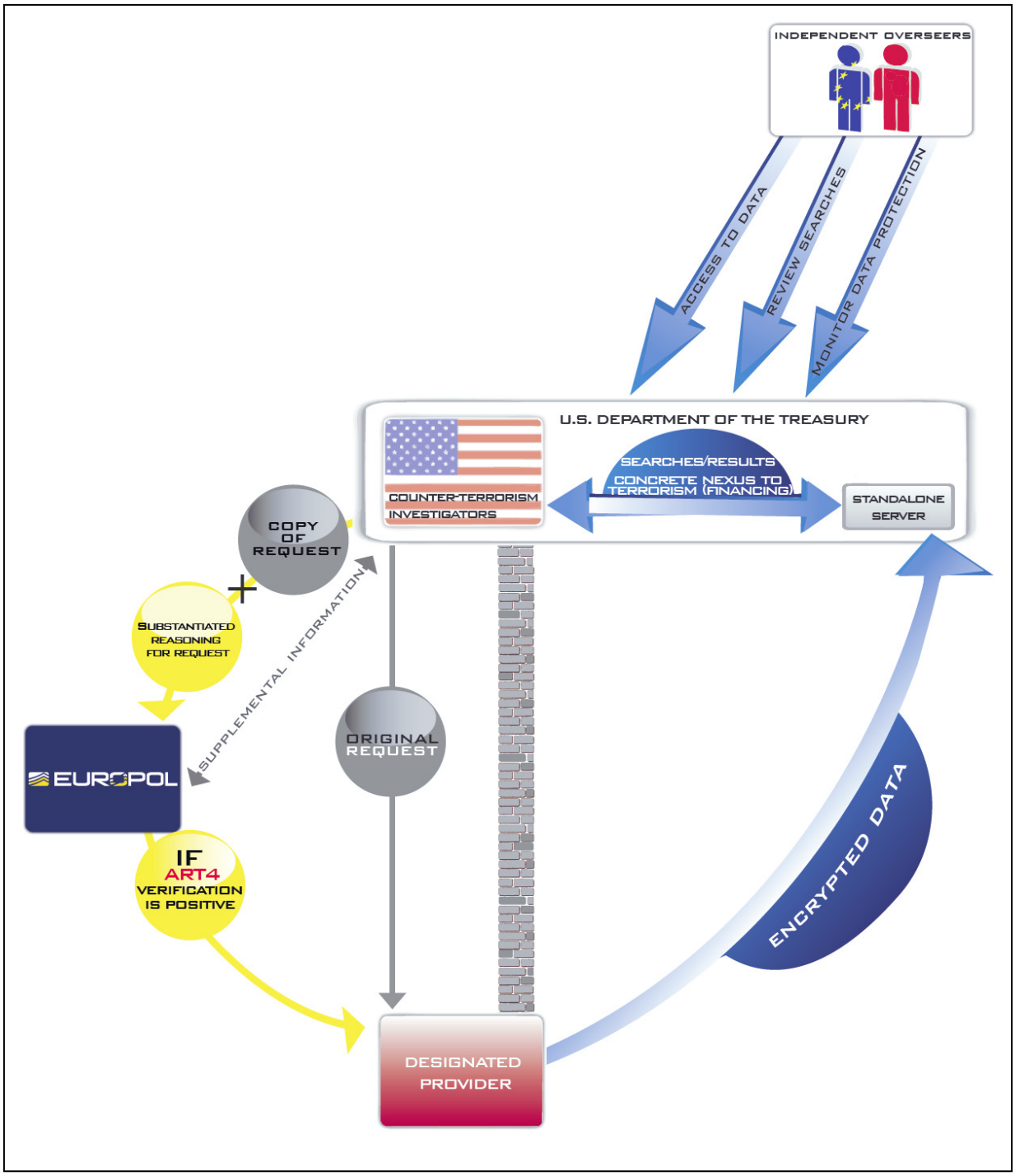
Article 4 of the TFTP Agreement gives Europol the task of verifying whether the requests from the responsible US authorities, to obtain financial messaging data stored in the EU by the Designated Provider, comply with specific criteria. In particular, the requests, together with any supplemental documentation, shall:

- Identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing;
- Clearly substantiate the necessity of the data;

- Be tailored as narrowly as possible in order to minimise the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat, and vulnerability analyses; and
- Not seek any data relating to the Single Euro Payments Area (SEPA).

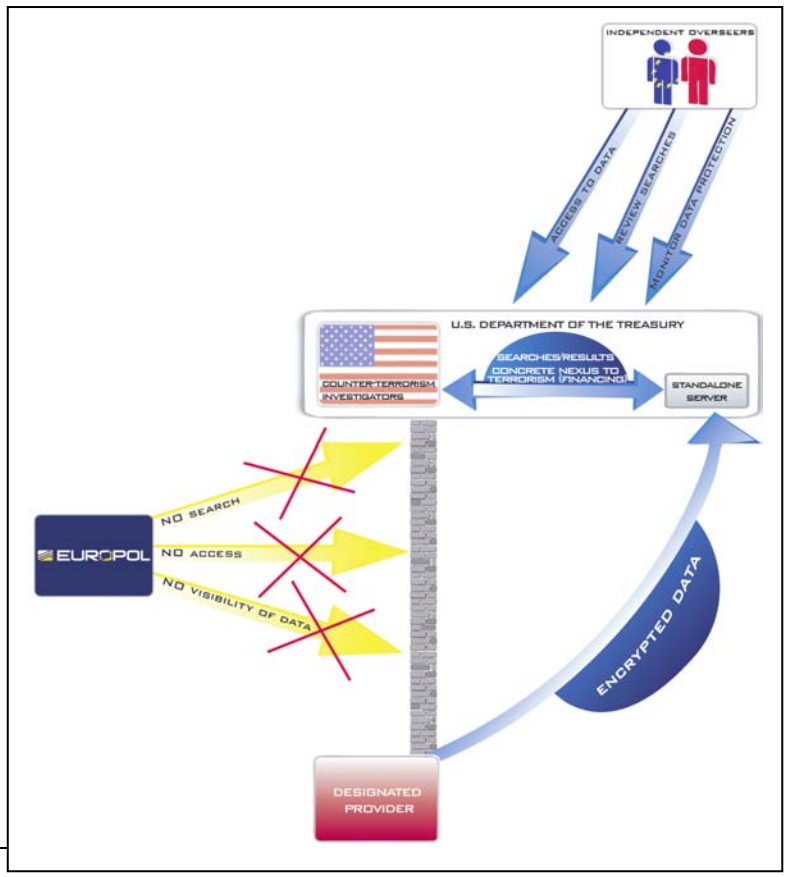
Article 4 also provides the framework within which US requests shall be considered. Requests are transmitted directly to the Designated Provider, with a simultaneous copy and any supplemental information provided to Europol for the purposes of carrying out its verification role. Europol informs the US Department of the Treasury and the Designated Provider of the result of its verification consideration. In the event of a positive verification, the relevant data is transferred directly from the Designated Provider to the US Department of the Treasury. No data is transmitted via, or copied to, Europol.

The following diagram illustrates this process.



In order to clarify Europol's role in relation to Article 4 of the TFTP Agreement, the following factors are highlighted:

- The provisions of the Agreement impose on Europol a task of verifying that each request reflects the principle of proportionality enshrined in Article 4 (2), based on an operational judgment of the validity of the request ("… taking due account of past and current terrorism risk analyses …" etc). Europol uses its expertise and knowledge in combating terrorism and the financing of terrorism, and its experience of operating principles of proportionality in its daily work of processing personal data, in order to make these judgments.
- Article 4 regulates the transfer of bulk data from the Designated Provider (based on standardised data categories) to the US Department of the Treasury, as clearly understood during the negotiation of the Agreement.[1] Strictly within the context of Article 4 the provisions aim at transferring information on a bulk and generic level according to the criteria established (limited in geographical scope, time period, and list of data categories). Identifying a nexus to terrorism in specific cases is a requirement under other provisions in the Agreement and forms no part of the request as submitted by the US Department of the Treasury to the Designated Provider under Article 4. These requests, therefore, do not contain details of individual data subjects. The substantiated reasoning for the request (which is sent to Europol to carry out its operational verification under Article 4, but not to the Designated Provider) occasionally includes personal data in the context of past and current terrorism risk analyses and investigations, for example with general references to Osama Bin Laden.
- Europol does not see or manage the provided data, which is transmitted directly from the Designated Provider to the US Department of the Treasury.
- Outside the framework of Article 4 the Agreement contains specific data protection safeguards that are applied after the transfer of the data to the US authorities and once individual searches of the provided data are initiated by the US Department of the Treasury. These safeguards are outlined, notably, in Articles 5, 6, 7, 8, 12, 15, and 16 and provide a comprehensive data protection regime, including through the establishment of the function of independent overseers. These provisions, inter alia, do not allow Europol to access the provided data.



[1] For example by the European Data Protection Supervisor (EDPS) in his press release and opinion published on 22 June 2010, www.edps.europa.eu

2.3. Europol's tasks concerning Articles 9 and 10 of the TFTP Agreement

Upon receipt of information provided by US authorities pursuant to Article 9 of the TFTP Agreement, Europol searches the data against all Europol information processing systems in order to identify possible connections with investigations in the EU. In the event of a hit the relevant competent authorities of the Member States are informed.

In regard to Article 10 (EU requests for TFTP searches) Europol has established a Single Point of Contact (SPOC) for its operational partners in the EU in order to make optimum use of this provision. It also submits search requests to the US in respect of its own analysis work.

3. Implementation of the TFTP Agreement by Europol

3.1. Background

The TFTP Agreement was negotiated by the European Commission, over a short period of time, on the basis of a negotiating mandate given by the Council. Following subsequent approval by Council and the European Parliament (EP) the Agreement entered into force on 1 August 2010, less than five weeks after the signatories of the European Union (EU) and the United States of America (USA) had concluded the final text of the TFTP Agreement.[2]

During this short time period Europol established the necessary administrative and other internal procedures to assume this new function. These arrangements were made on the basis of an agreement between the European Commission and the US regarding the "technical modalities necessary to support the Europol verification process", a condition laid out in Article 4 (9) of the TFTP Agreement. A copy of this agreement is attached to this information note. These modalities were agreed and adopted on 28 July 2010, 3 days before the TFTP Agreement entered into force.

3.2. Organisational set-up

In line with the principles set out in the "technical modalities" document, Europol established a dedicated unit (TFTP Unit within the Operations Department of Europol – "Unit O9") to carry out the tasks under the TFTP Agreement. The unit consists of three (3) qualified, trained and vetted staff members (with an appropriate background in, and understanding of, counter terrorism and terrorist financing) who discharge the duties assigned to Europol under the Agreement. They are supported and advised by dedicated officials in the Legal Affairs Unit, Data Protection Office and Security Unit of Europol.

Given the sensitivity of the programme and the information involved, additional security measures were established at Europol for this unit's work.

In addition, on 30 July 2010, Europol opened a dedicated Analysis Work File (AWF) to process the concerned data sent by the US under Articles 9 and 10 of the TFTP Agreement. This data is protected by Europol's robust and tested data protection regime.

3.3. Processing of Article 4 requests

In line with the agreement on "technical modalities" Europol devised and implemented a detailed process description to manage the procedural steps involved in discharging its responsibilities under the TFTP Agreement. After the first six months of operating this process and, taking into account advice from the Joint Supervisory Body (JSB) and an earlier request by the US to enhance the applicable security regime, Europol comprehensively reviewed the process. A revised version was adopted and introduced in March 2011.

The procedural steps involved in the process include specific actions to assess the validity of the US request in terms of its compliance with the criteria established in Article 4, including a record of the verification officer's operational judgment and a record of the advice given by the Legal Affairs Unit and Data Protection Office (DPO). The DPO has seen every request since the Agreement entered into force, but following observations made by the JSB, Europol decided to make certain practical enhancements to the process to ensure a more efficient involvement of the DPO.

[2] Official Journal of the European Union (OJEU), L 195/5 – L 195/14, published on 27 July 2010

As part of the process, a standard template is used as a formal record of the advice from each party and of the authorising officer's final decision.

3.4. Classification of Article 4 requests under the TFTP Agreement

Europol only classifies information when necessary to protect the legitimate interests of Member States, Europol's cooperation partners or the organisation itself. When the TFTP Agreement entered into force on 1 August 2010 Europol classified the handling of US requests at the level of "RESTREINT UE/EU RESTRICTED", partly in view of technical limitations in the secure information exchange system between Europol and the US. Given the speed with which the Agreement entered into force, no time was available to establish a dedicated communication system, in spite of significant security concerns surrounding the programme. Three months later Europol and the US reviewed these and other handling measures, taking into account especially the leaking of a sensitive document describing the "technical modalities" of Article 4 and its publication on an internet site in Germany. This led to the responsible US authorities, on 5 November 2010, formally requesting Europol to regard all US information in relation to its Article 4 requests as carrying a classification standard in the US, which is the equivalent of "SECRET UE/EU SECRET". The US authorities judged that unauthorised disclosure of information related to the requests would significantly undermine US and European counter-terrorism efforts, taking into account the high operational sensitivity of information included in supplemental documents relating to the requests.

After carrying out its own risk assessment Europol came to the same conclusion. Regardless, Europol is legally bound to apply a level of protection equivalent to the one applied by the US authorities, in line with a universal security principle of respecting the security requirements of the data owner and in accordance with the provisions of the extant cooperation agreement between Europol and the US.

Since November 2010, therefore, Europol has classified all material relating to Article 4 requests as "SECRET UE/EU SECRET", including that received in the period before. US requests are now routinely classified as "US SECRET" and routed to Europol through secure diplomatic channels.

Europol has an institutional capability to handle classified data in accordance with a framework laid down in the Europol Council Decision and Europol Security Manual. The measures involved are consistent with those applied in Member States and EU institutions. These include measures to limit access to such information. Importantly, however, the decision to upgrade the security of these documents had no bearing on the privileges and rights of the JSB, which enjoys unrestricted access to all information stored at Europol, regardless of classification.

3.5. Composition of Article 4 requests under the TFTP Agreement

The set of documents supporting the verification process at Europol comprises:

- A cover letter from the US Department of the Treasury;
- A copy of the request submitted by the US Department of the Treasury to the Designated Provider, setting out the:
    - Geographical sphere (list of countries) and the relevant period to which the request refers;
    - List of data categories the US authorities are seeking to retrieve (from the full repository of financial transactions processed by the Designated Provider).
- A set of documentation which constitutes the substantiated reasoning for the request (sent only to Europol and not to the Designated Provider), outlining:
    - Reasons (based on analysis findings and results from investigations) for the selection of the geographical sphere (list of countries) and data categories referred to in the request;
    - An overview of current and past terrorism investigations carried out by US authorities, mentioning targets of investigation including personal data.

Due to the specific construction of the TFTP Agreement the US authorities must demonstrate a concrete nexus to terrorism in individual cases only in the context of the individual searches under Article 5 (5) of the TFTP Agreement, once the received data are used for concrete search and/or analysis activities etc. Consequently, Article 4 (2) of the TFTP Agreement does not prohibit that the requests received by Europol exhibit a certain level of abstraction.

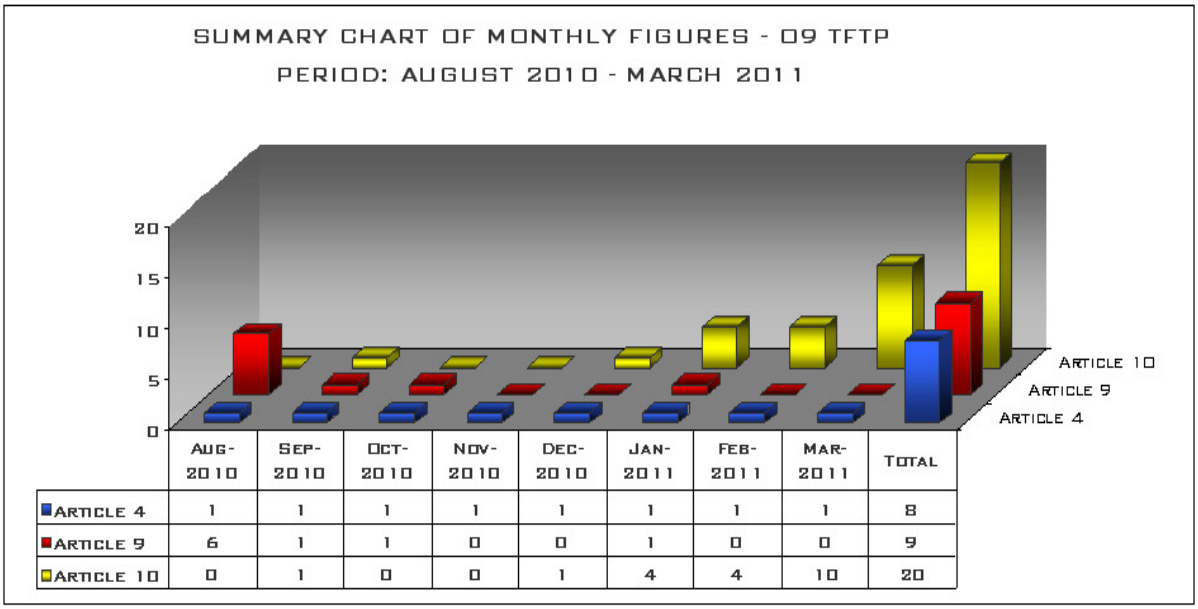
Nonetheless the information package provided to Europol by the US authorities, in support of its requests, is substantial and well documented, running to an average of 56 pages per request. By the time Europol has completed its internal assessment of the request and recorded all available judgments and advice the whole package runs to an average 67 pages. The most recent contains over 80 pages, reflecting efforts by the US in recent months to provide a greater amount of information to substantiate its requests.

The request usually covers a period of 4 weeks. Europol has only received one request covering a longer period. It should be borne in mind that the TFTP Agreement specifies neither a minimum nor a maximum period of time per request.

In relation to the clause of Article 4 (2), according to which Single Euro Payments Area (SEPA) data are excluded from the request, Europol confirms that, so far, every US request specifically states that no SEPA data is requested. The EU review undertaken under Article 13 of the TFTP Agreement highlights that the Designated Provider also confirmed that no SEPA related data have been provided to the US authorities.

3.6. Statistics: Number of requests/other information received by Europol

The number of requests Europol has managed up to April 2011 is shown below:



	AUG-2010	SEP-2010	OCT-2010	NOV-2010	DEC-2010	JAN-2011	FEB-2011	MAR-2011	TOTAL
ARTICLE 4	1	1	1	1	1	1	1	1	8
ARTICLE 9	6	1	1	0	0	1	0	0	9
ARTICLE 10	0	1	0	0	1	4	4	10	20

It is clear from the development of the figures that the information requests from the EU towards the US authorities, making use of Europol's central EU information hub capabilities, has considerably increased over the last eight (8) months. It should be noted, though, that Member States also route information requests bilaterally to the US.

In terms of the spontaneous provision of information by the US to the EU, under the terms of Article 9 of the Agreement, Annex 1 to the EU review report confirms that a total of 84 reports were issued by the US to EU Member States and EU authorities in the first six months of the implementation of the Agreement. Nine of these were routed through Europol and have been the subject of further operational development in the EU in some cases. In one notable case, the information provided has supported an ongoing, high profile investigation involving several countries in Europe and elsewhere, leading to action including judicial measures. This investigation continues so its details are not suitable for public disclosure at this stage.

3.7. Further details concerning Article 4 requests

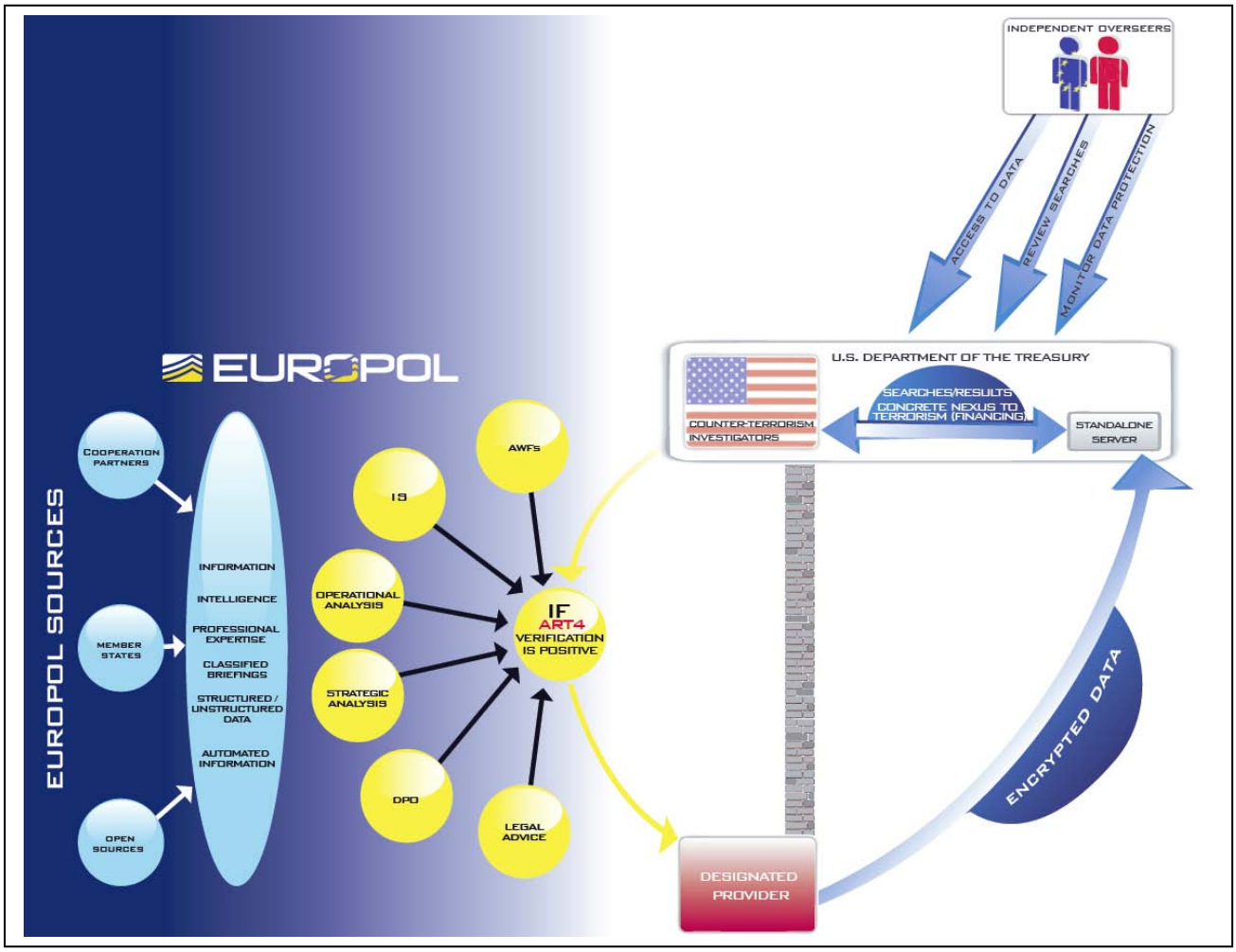
Europol has received eight (8) written requests from the US to date and, following careful scrutiny in each case, has verified all of them. All verification decisions have been based on a fully documented, rigorous examination of formal requests submitted by the US Department of the Treasury.

In five (5) out of eight (8) Article 4 requests received to date, Europol has requested and received from the US additional written information in order to allow Europol to better understand the operational context of the individual request. In six (6) of the cases Europol has failed to meet the time period of 48 hours allocated to the task of verification in the "technical modalities" agreement, taking 16 days to complete its work in one case. This occurred notwithstanding the availability of sufficient resources and a very high commitment to the task. Instead it is a reflection of the care and diligence Europol has applied in discharging its responsibilities under Article 4, in particular by ensuring it receives all necessary information from the US.

In line with the criteria to "minimise the amount of data requested", Europol confirms that the scope of the requests is limited in terms of geography and the number of data categories listed. With regard to the latter, the scope has been narrowed further recently following an internal review by the US Treasury Department. It must be noted, however, that Europol does not have access to the data sent to the US by the Designated Provider (see section 2.2 of this report) and, therefore, is unable to quantify the level of actual data transferred.

In assessing each request, in order to reach a verification decision, Europol relies on the full range of information and other sources available: Analysis Work Files (AWFs), which are among the most valuable databases of organised crime and terrorist activity in the EU, the Europol Information System (IS), operational and strategic analysis in relation to specific terrorist threats and individual operations, the professional expertise of dedicated counter-terrorist officers, and the advice of the Legal Affairs Unit and Data Protection Office (DPO).

The following diagram provides an overview of the sources available to Europol in arriving at its verification decision:



In addition to the extensive written documentation provided in connection with each request, the US authorities have provided Europol with three classified oral briefings, setting out the context and current focus of US counter-terrorist activities. These have included specific information about ongoing international counter-terrorist operations. This information is one important element for Europol in reaching an informed understanding of the US counter-terrorist programme and, therefore, the context in which US requests are submitted. However, in the context of the specific provisions of Article 4 these oral briefings do not take the place of the formal written documentation submitted. Europol accepts the recommendations made in the EU Review and JSB Inspection Reports that Article 4 requests should be judged on written, auditable material.

A detailed overview of the statistics for all Article 4 requests operated by Europol under the TFTP Agreement is attached to this Information Note.

4. Joint Review – Article 13 of the TFTP Agreement

4.1. Background

Article 13 of the TFTP Agreement foresees that a joint review is carried out by the Commission and the US authorities to assess the status of implementation of the Agreement, in particular the aspect of compliance with the data protection obligations laid down in the Agreement. The EU review report was published by the European Commission on 17 March 2011. On the same day Commissioner Malmström presented its findings to the LIBE Committee. The review team comprised officials from the European Commission, two representatives from national data protection authorities of EU Member States, and a judicial expert from Eurojust.

4.2. Main findings

In terms of the findings relevant to Europol, the EU review report concludes that:

- "the EU review team is satisfied that the procedures required under the agreement have been put in place to ensure that, in principle, the requests for information are tailored as narrowly as possible, and are also in line with the other requirements of the Agreement.
- "Europol clearly takes its role under the Agreement very seriously, and has put in place all the necessary elements to fulfil its role in accordance with the Agreement and its implementing technical modalities".

Regarding the classified briefings from the US authorities, the EU review report states that:

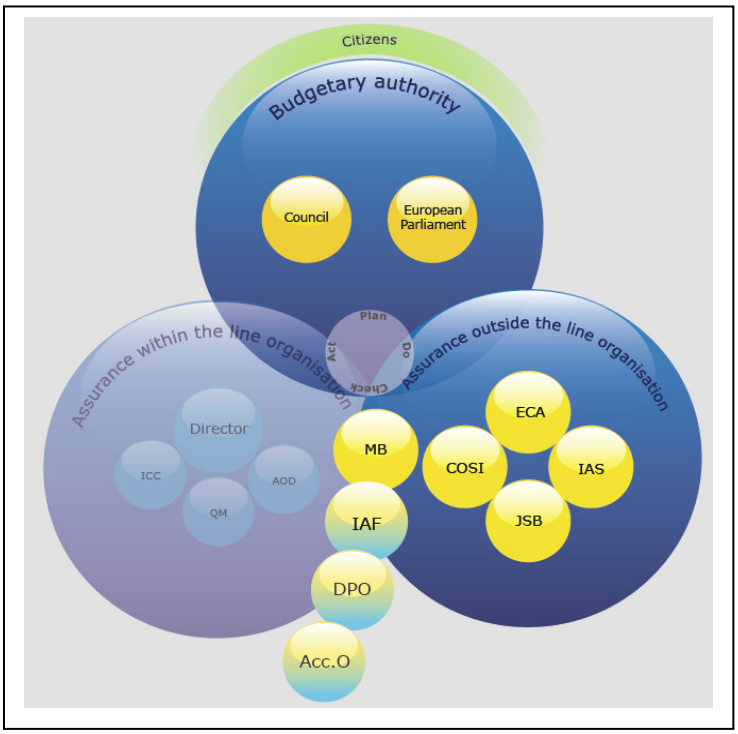
"The EU review team recommends that as much (classified) information as possible substantiating the requests is provided to Europol in a written format in order to support it in its tasks under Article 4 and to allow for more effective independent review."

Commissioner Malmström underlined these aspects in her press statement on the EU review report as well, stating that "the review confirms that Europol has taken this task very seriously, and has put in place the necessary procedures to execute it in a professional manner and in accordance with the agreement".

5. JSB inspection on the TFTP Agreement

5.1. Background

On 11 November 2010, the Joint Supervisory Body (JSB) conducted an inspection on the implementation of the TFTP Agreement by Europol. The role of the JSB seeks to ensure that the data protection responsibilities assigned to Europol, in particular in the Europol Council Decision (ECD)[3], are observed and the attendant processes improved, where necessary.



Apart from the EP and Council with their distinct functions, the JSB is, along with the European Court of Auditors (ECA), the Internal Audit Service (IAS) of the Commission, the Standing Committee on Operational Cooperation on Internal Security (COSI), the Europol Management Board (MB), the Internal Audit Function (IAF), the Data Protection Officer (DPO) and the Accounting Officer (Acc.O), one of the assurance providers in the governance and oversight framework of Europol. This is a robust and well-developed governance architecture.

Europol has a close and enduring relationship with the JSB, established over 12 years. Its inspectors are regular visitors to Europol, offering advice and support on a range of issues relevant to the agency's operational work. With the support of the JSB Europol has established one of the strongest reputations in the world for applying data protection safeguards in a police environment. The arrangements involved continue to improve. The most recent annual inspection of Europol by the JSB, an exhaustive study of Europol's data processing activities carried out in 2010, was probably the most positive report of Europol's compliance with data protection standards ever recorded by the JSB.

During the inspection by the JSB regarding the TFTP Agreement, the JSB had access to all documentation processed by Europol, including the original Article 4 requests, which are classified as "SECRET UE/EU SECRET". Following the inspection in November 2010, a draft Inspection Report was submitted to Europol on 8 February 2011. Europol replied with comments on the draft on 18 February 2011. The final Inspection Report was received at Europol on 4 March 2011 and its classified annex, on 18 March 2011.

5.2. The recommendations contained in the JSB Inspection Report

In its report, the JSB does not doubt the validity of the role ascribed to Europol in the TFTP Agreement or the fulfilment of its responsibilities under the Agreement but makes five recommendations to improve Europol's implementation of Article 4. On 15 March 2011, Europol submitted a letter to the JSB Chair confirming Europol's acceptance of all five recommendations and detailing work already underway or completed in respect of all them. A copy of this letter is attached to this Information Note.

The Chairperson of the JSB outlined some aspects of Europol's reply in the session with the LIBE Committee on 16 March 2011.

[3] Official Journal of the European Union (OJEU), L 121/37 – L 121/66, published on 15 May 2009

The JSB Final Inspection Report was also discussed during the last Europol Management Board (MB) meeting held on 23–24 March 2011, in the presence of the Chairperson of the JSB. The Europol MB came to the conclusion that Europol has discharged its responsibilities as foreseen by the TFTP Agreement and implemented the necessary provisions correctly. It also endorsed the implementation of the JSB recommendations by way of making further improvements.

The key recommendation in the Final JSB Inspection Report seeks to motivate the US Department of the Treasury to provide even more written documentation to Europol to carry out its verification role under Article 4. This is very similar to the findings and recommendations recorded by the EU review team (see section 4.2 above).

On 30 March 2011 Europol officials held a workshop with the JSB to discuss the implementation of this and the other recommendations. At the heart of the discussion are some conceptual issues regarding the application of proportionality principles concerning the criteria laid out in Article 4, in particular the extent to which these relate to data protection or operational judgments, or a combination of both. Europol has strictly followed the interpretation of the Agreement clarified by the European Commission and the US, and confirmed by the Europol MB. This characterises the test of necessity under Article 4 as one relating to operational considerations.

During the process of implementing the Agreement over the first six months the JSB and, to a lesser extent, the Data Protection Officer of Europol, have held a different opinion on this point. In keeping with a long tradition of both parties working together informally to arrive at the best position, particularly in respect of complex issues, the workshop between Europol and the JSB on 30 March 2011 aimed to resolve these differences. Progress was made, in particular in terms of identifying concrete, further improvements to the recording components of the verification process. This will be discussed further at another workshop in May 2011 and also with US authorities.

6. Concluding remarks

Notwithstanding the very short time Europol had to prepare for its new responsibilities under the TFTP Agreement, and the application of the provisions of Article 4 especially, Europol believes it has discharged its responsibilities with great care and to a high professional standard. The EU review team, Commissioner Malmström, and the Europol Management Board, have all arrived at the same conclusion. However, further improvements to Europol's activities are necessary in line with the recommendations of the EU review report and JSB Inspection Report. These recommendations are the subject of high priority attention by Europol.

Meanwhile public discourse on this subject, including in the LIBE Committee, has identified a number of apparent concerns, particularly in regard to the appropriateness of Europol's verification role under Article 4 of the TFTP Agreement, the level of scrutiny applied to US requests, and the transparency of Europol's activities in regard to the implementation of the Agreement.

Europol hopes that this detailed Information Note assists in clarifying any issues about Europol's role and its activities in implementing the Agreement. In particular it offers evidence of Europol operating a comprehensive and robust process to assess and verify US requests strictly in accordance with the Agreement.

On the important question of transparency, substantial information has been released publicly in this note beyond a level normally applied to Europol's operational activities. This reflects the unusually high level of public sensitivity attached to the TFTP Agreement and Europol's desire to operate in a transparent and accountable manner. The only relevant information remaining undisclosed are operational details, the public disclosure of which would seriously undermine Europol's reputation as a reliable law enforcement agency and the effectiveness of US and EU counter-terrorist activities.

7. Annexes

7.1. Annex 1: "Technical modalities" – Article 4 (9) of the TFTP Agreement

Technical modalities for the Europol verification process with regard to 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 the Purposes of the Terrorist Finance Tracking Program (TFTP) ("Agreement")

Introduction

This paper is intended to set out the technical modalities referred to in Article 4 (9) of the Agreement in order "to support the Europol verification process", and to identify the different steps and elements of this verification process with respect to data that is stored in the territory of the European Union and sought under the terms of the Agreement.

The modalities may be subject to modifications, as necessary, once the Europol verification process is in place. Such modifications are to be jointly coordinated by the Parties to the Agreement.

Main implementation components

a) Distinct and dedicated unit within Europol, under appropriate supervision and with the involvement of the Data Protection Officer of Europol

Europol intends to establish within its Operations Department a distinct and dedicated unit regulated and supervised pursuant to the existing legal framework and current organisational arrangements within Europol. The requirements for this unit include appropriately experienced and vetted staff with a background in and understanding of counter terrorism and terrorist financing. The U.S. Treasury Department intends to provide appropriate training and background information on the TFTP and the context in which the U.S. Treasury Department makes its production orders ("Requests") to the Designated Provider so that the unit acquires the necessary understanding of the functioning of the program to carry out its task of verification as set out in Article 4 (2) of the Agreement.

The unit should be physically located in a distinct part of the Europol building, which currently houses the Counter-Terrorism Unit of Europol and which already benefits from enhanced physical security measures.

Within Europol the Data Protection Officer is competent to ensure compliance with the applicable data protection legal framework established in the Europol Council Decision[4] whenever U.S. Treasury Department Requests or supplemental documents make reference to identified or identifiable natural persons.

b) Elements needed for the verification

The U.S. Treasury Department intends to provide explanatory elements to aid Europol's understanding of the Requests, including information on an historical basis

[4] Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ L 8, 12.1.2001, p. 1.

identifying specific counter terrorism cases where TFTP-derived information has been supplied. The U.S. Treasury Department Request should be accompanied by sufficient explanatory elements for the selected staff to make an informed assessment of whether a Request complies with the requirements of Article 4 (2) of the TFTP Agreement.

It is intended that certain explanatory elements are to be provided in the form of supplemental documents accompanying the Request. The supplemental documents should substantiate the continuing necessity of the data to be provided.

They should provide a justification for the Request, including for the types or categories of messages contained therein, as well as for any widening of the geographical scope of a Request. The justification provided should result from terrorism risk, geographic threat or vulnerability analyses. The terrorism risk, geographic threat and vulnerability analyses should be appropriately identified and explained.

The explanatory elements should also include briefings by the U.S. Treasury Department for designated Europol staff on a regular basis in order to further facilitate the verification process.

c) The normal duration of the verification process

Article 4 (4) of the TFTP Agreement specifies that Europol is to complete its verification "as a matter of urgency." In the event that sufficient information is available to Europol to make an informed assessment of the compliance of the Request with Article 4 (2) of the Agreement, the verification process should be completed within 48 hours.

In those cases where Europol considers the information provided to be insufficient to allow verification, Europol should ask for additional information from the U.S. Treasury Department.

In the event that Europol considers that the Request does not comply with Article 4 (2) or that, after receiving additional information from the U.S. Treasury Department, Europol continues to believes that the information provided is not sufficient to allow verification, before taking a negative decision Europol should consult with the U.S. Treasury Department to address any remaining matters of concern.

d) Security and Confidentiality arrangements

It is intended that the regime of data security set out under Europol Council Decision article 35 is to apply to the verification process.

On the technical level, there is a requirement for a secure means of transmission between the U.S. authorities and the TFTP Unit at Europol. Europol has a Liaison Office in Washington. It is connected to Europol HQ on the secure SIENA network. This is the principal secure law enforcement connection used by EU Member States to exchange intelligence in the Europol environment. It is accredited to EU RESTRICTED. The TFTP Request is categorized by the U.S. authorities as LAW ENFORCEMENT SENSITIVE and, therefore, SIENA offers an appropriate security framework for the transmission of such Requests.

If additional measures are required to transmit any information of a higher classification standard, specific encryption solutions should be made available.

In addition to the enhanced level of physical security that the TFTP Unit should have and the secure means of transmission from the U.S. Treasury Department to Europol HQ, the following measures are envisaged by Europol.

The TFTP Unit should be staffed by Europol officers who hold agreed levels of security clearance and who are specifically designated and authorised to handle TFTP material. Only designated and authorised Europol officers should have access to the

secure area within which a TFTP Request is to be processed. Only designated and authorised Europol officers should handle and process the TFTP Requests and any "supplemental documents" or other "explanatory elements." Like all other members of Europol staff, these officers are bound by a duty of discretion and confidentiality. Europol will brief the US Treasury Department on the implementation of its confidentiality arrangements and on any changes to them thereafter.

In addition, no information transmitted by the U.S. Treasury Department, including information regarding types or categories of messages, is permitted to be shared either with EU Member States or with other parties without the express written authorization of the U.S. Treasury Department.

In order to notify the Designated Provider that the Request of the U.S. Treasury Department has been verified and is found to comply with Article 4 (2), a secure communication channel between Europol and the Designated Provider should be established.

A risk assessment should be carried out in order to define controls to be implemented regarding the necessary communication with the Designated Provider, taking into account Europol's requirements.

e) The form and motivation of the decisions to be adopted under Art. 4

Once the verification process is completed, Europol should record its decision in writing with justifications. If the decision is positive, i.e., the compliance of the Request with Article 4 (2) of the Agreement is confirmed, Europol should immediately notify the Designated Provider by the agreed route that the Request complies with the Agreement according to Article 4 (4). Europol should, at the same time, inform the U.S. Treasury Department.

After completing the evaluation process outlined above, in the event that Europol determines that it cannot confirm that the Request complies with Article 4 (2), Europol should immediately notify the Designated Provider by the agreed route that the verification has not been successfully completed. A copy of this notification should, at the same time, be sent to the European Commission and the U.S. Treasury Department.

f) Point of contact

Europol, the European Commission, and the U.S. Treasury Department should each identify a point of contact to coordinate the application of these technical modalities, and also should request the Designated Provider to identify a point of contact. These points of contact should communicate directly with one another for the purposes of these technical modalities. Each may change the designated point of contact upon written or electronic notification thereof to the others.

7.2. Annex 2: Statistics regarding the handling of Article 4 requests

Summary of statistics for Article 4 requests under the TFTP Agreement:

Period	01 August 2010 – 31 March 2011				
Month	Article 4 request		Request for supplemental information and reply		
	Date of receipt	Number of pages	Yes/No	Date of request	Date of reply
Aug-10	06/08/2010	51	Yes	06/08/2010	09/08/2010
Sep-10	08/09/2010	51	No	-/-	-/-
Oct-10	05/10/2010	53	Yes	06/10/2010	08/10/2010
Nov-10	02/11/2010	55	Yes	03/11/2010	03/11/2010
Dec-10	22/12/2010	58	No	-/-	-/-
Jan-11	07/01/2011	58	No	-/-	-/-
Feb-11	14/02/2011	58	Yes	15/02/2011	17/02/2011
Mar-11	09/03/2011	63	Yes	09/03/2011	22/03/2011
		56 (Average)			

Overview regarding verification communication and total set of documentation:

Period	01 August 2010 – 31 March 2011		
Month	Communication with the Designated Provider		Total set of verification documentation (including DPO advice, verification decision)
	Delay notification	Verification	Number of pages
Aug-10	06/08/2010	10/08/2010	66
Sep-10	10/09/2010	14/09/2010	61
Oct-10	07/10/2010	08/10/2010	65
Nov-10	-/-	04/11/2010	61
Dec-10	-/-	23/12/2010	64
Jan-11	07/01/2011	10/01/2011	64
Feb-11	16/02/2011	17/02/2011	74
Mar-11	11/03/2011	25/03/2011	86
			67 (Average)

7.3. Annex 3: Letter to the JSB: Implementation of JSB recommendations

EUROPOL

The Hague, 15 March 2011

DIRECTOR

Chairperson of the Europol
Joint Supervisory Body (JSB)
Ms Isabel Cruz
Rue de la Loi 175
Bureau 0070FL59
B-1048 Brussels
By email

Implementation of the Terrorist Financing Tracking Program (TFTP) Agreement

- Final JSB Inspection Report in relation to the implementation of the TFTP Agreement by Europol, JSB/Ins. 11-07
- Invitation to discuss open issues regarding the implementation of the TFTP Agreement (in particular Article 4 of the TFTP Agreement)

Dear Isabel,

Following our telephone conversation yesterday, I hereby invite the JSB to attend a workshop with Europol officials on the subject of the implementation of the EU–US TFTP Agreement.

This workshop would address the findings of the JSB Inspection Report and seek to identify concrete measures to implement its recommendations, taking into account also the findings of the Joint Review Report, referred to in Article 13 of the TFTP Agreement, to be published shortly by the European Commission. Furthermore, in so far as different viewpoints still exist between the JSB and Europol on the requirements and modalities of the verification responsibilities outlined in Article 4 of the Agreement, this could also be addressed in the workshop.

Given the sensitivity of the TFTP Agreement and its importance to Europol, I attach a very high priority to ensuring Europol reaches a common understanding with the JSB on the issues raised in the Final Inspection Report. As you know some of these issues have received adverse public attention recently in a way that has undermined the reputation of Europol. On an urgent basis I wish to repair this damage and take steps to ensure that it is not repeated.

Given the issues involved and the fact that the implementation of the TFTP Agreement continues meanwhile I would like to conduct this work as soon as possible. I would be grateful, therefore, if you would consider nominating JSB members to attend a workshop at Europol in the week beginning 28 March 2011 or as soon as possible thereafter. Daniel Drewer in the Europol Data Protection Office is available to coordinate meeting arrangements with your staff.

2566-563 (534309v4)

Raamweg 47
2596 HN The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 302 58 96
www.europol.europa.eu

In the meantime I am pleased to attach, for your information, a status report on the work already completed by Europol to implement the five recommendations in the Final Inspection Report. As I have previously reported to you Europol began addressing all of them, on a high priority basis, as soon as they were identified during the course of the inspection visit last year. Significant work has now been completed in respect of all the recommendations. I am sure this will form a helpful basis on which our respective teams could consider even further improvements, as necessary.

I am convinced by the enduring strength of the relationship between Europol and the JSB, developed over many years. I am sure it will grow further through our joint work on this file.

Yours sincerely,

Rob Wainwright
Director

Overview of actions taken by Europol: Final Joint Supervisory Body (JSB) Inspection Report (JSB Ins. 11/07)

Recommendation N° 1
Inform the JSB on the results of the review of policies and procedures related to Europol's tasks under the TFTP Agreement
Background information
Europol put in place a robust and detailed process to implement the TFTP Agreement from the first day of its applicability, and in particular concerning the verification of the requests under Article 4 of the TFTP Agreement. The process description, setting out the required procedural steps to ensure compliance with the provisions of the TFTP Agreement, had been finalised by the time the JSB inspection took place on 11 November 2010. The completed process description was available to the JSB during the visit to Europol. The process (description) was under review at the time of the JSB inspection, given that the responsible US authorities had asked, on 5 November 2010, for an enforced security regime concerning the operation of Article 4 requests, stating that unauthorised disclosure of the related information would significantly undermine US' and European counter-terrorism efforts.
Action taken by Europol – Recommendation addressed
A new version of the process description, setting out the refined sequence of steps to discharge the responsibilities under the TFTP Agreement, in particular regarding Article 4, has now been finalised, bearing in mind the request from the US authorities at the end of last year to arrive at an enforced security regime (which led to the classification of Article 4 related information as "EU SECRET"). As part of the new process description, also a new version of the verification template (constituting the record for the verification decisions under Article 4 of the TFTP Agreement) has been devised. Technical considerations (for the transmission of Article 4 requests from the US authorities to Europol) needed to be clarified before the process description could be completed. The process description will be available to the JSB for the planned workshop at Europol.

Recommendation N° 2
Ensure the ability of the Europol Data Protection Officer to carry out his role, particularly in view of the short period of time in which Europol is expected to react to requests received under Article 4 of the TFTP Agreement
Background information
The Data Protection Officer (DPO) was consulted and closely involved in the elaboration of the new version of the process description, including the new template to record the verification decisions in relation to Article 4 of the TFTP Agreement.
Action taken by Europol – Recommendation addressed
The new version of the process description reinforces the engagement of the Europol DPO in the handling of requests under Article 4 of the TFTP Agreement, leading to an even closer involvement of the DPO upon receipt of the requests under Article 4 of the TFTP Agreement, the submission of requests for receiving supplemental information from the US authorities, and the decision on the verification before it is communicated to the concerned US authorities.

The new version of the verification template also contains now a separate section, in which the references of the advice from the DPO on the matter are recorded, prior to the final section for the Authorising Officer to document the decision in relation to the verification of the request under Article 4 of the TFTP Agreement.

Recommendation N° 3
Ensure hard-deletion of Article 4 data which were inputted into some of Europol's information processing systems (iBase and SIENA) before the upgrading of the security level.
Background information
All concerned Article 4 related data were deleted from the relevant IT systems, following the decision of 5 November 2010 to classify Article 4 related requests as "EU SECRET" which also led to a reclassification of all Article 4 requests and the related information since the entry into force of the TFTP Agreement. However, Europol understands that the JSB seeks to ensure that also potential 'back-up' storage of the deleted data is erased from the concerned IT systems.
Action taken by Europol – Recommendation addressed
A new check of the concerned IT systems was initiated to ensure full compliance with the recommendation of the JSB. All Article 4 requests and the related information are now classified as "EU SECRET" – the details of the handling of the information are also set out in the new version of the process description. Europol considers the recommendation as addressed.

Recommendation N° 4
Contact the US Treasury Department to ensure that requests made under Article 4 of the TFTP Agreement comply with the criteria laid down in Article 4 (2) of the Agreement. Requests must contain more detailed information, specific to each request, in order to allow Europol to verify whether the requests comply with the requirements of Article 4 (2) of the Agreement. Taking into account the fact that - under the current TFTP Agreement - Europol receives copies of the requests sent to SWIFT by the US Treasury Department, certain additional information may need to be provided by the US Treasury Department to Europol in supplementary documents.
Background information
When fulfilling its duties under Article 4, Europol carries out an operational assessment of the US requests against the clear criteria of Article 4 and on the basis of information available to Europol. All verification decisions by Europol are based on a fully documented, rigorous examination of formal requests submitted by the US authorities. Article 4 of the TFTP Agreement does not require that the US have to demonstrate a concrete nexus to terrorism in individual cases, which is only asked for from the US Department of Treasury under Article 5 (5) of the TFTP Agreement. Consequently, Article 4 (2) of the TFTP Agreement does not prohibit that the requests have a certain level of abstraction or are similar in their wording. The fact that the requests have a similar geographical scope is equally not excluded by Article 4 and is supported by Europol's strategic analysis concerning perceived terrorism threats and vulnerabilities.

However, both the US authorities and Europol are aware that the requests submitted under Article 4 must be fully justified in terms of the criteria laid down in Article 4.
Action taken by Europol – Recommendation addressed
To date, Europol has received 8 requests from the US authorities in relation to Article 4 of the TFTP Agreement. In five (5) out of eight (8) requests, Europol sought additional, supplementary information in writing before taking a decision to verify the request in accordance with the criteria set out in Article 4 of the TFTP Agreement (the eighth verification decision is pending – a second request for supplemental information is being prepared). This underlines, from Europol's perspective, the great care and diligence the organisation applies in operating the Article 4 requests. Since the time of the JSB inspection visit last year, in particular, Europol has sought from the US additional information in support of the requests. The US has responded constructively to these requests and a trend towards more detailed information from the US is now visible. The planned workshop at Europol could assess this point. The requirement for the US to provide as much information as possible to support its requests was also directly raised by Europol during the process, led by the Commission, to prepare the Joint Review on the implementation of the Agreement. On 16 February 2011 the Europol Director wrote to the Commission asking it to specifically address this issue in the review.

Recommendation N° 5
Ensure that verifications are made based on the written requests - along with any supplemental documents - in order to allow proper internal and external supervision, by Europol's Data Protection Office and the JSB respectively.
Background information
Europol asks for supplementation information in writing (see above – Recommendation N° 4)
Action taken by Europol – Recommendation addressed
All verification decisions are made on the basis of a rigorous scrutiny of requests submitted by the US and all available supplementary information in writing. These decisions do not rely on any oral, unrecorded briefings. However, the classified briefings given by the US to Europol help to provide contextual information about the framework of the programme in the US and the operational use made of the transferred data. The new process description clarifies this position and underlines the importance of ensuring verification decisions are based on written requests.