The Hague, 28 May 2019

EDPS case number: 2018-0638

EDPS TFTP Inspection

05/02/2019 – 06/02/2019

1. Scope

The EDPS inspection team focused on Europol's compliance with Article 4 of the TFTP Agreement[1].

This inspection does not cover Europol's involvement according to Articles 9 and 10 of the TFTP agreement.

Furthermore, the assessment of the validity of the TFTP agreement as such is outside of the supervisory role of the EDPS.

2. Methodology

The inspection team examined the six most recent requests from the US Department of Treasury (US DoT) and Europol's analysis contained in the respective verification forms, covering the period August 2018-January 2019.

Based on the workflow description, the EDPS inspection team carried out interviews with all actors involved in Europol's verification process: the Head of TFTP team - Unit 46 (Verification Officer – operational analysis), Head of Business Area Corporate Governance (procedural compliance), Head of the Europol Counter Terrorism Centre (Authorising Officer) and with members of the Data Protection Function.

The EDPS inspection team also discussed the overall process of handling TFTP-related documents. To that end, interviews were conducted with the Head of team TFTP, a C1 staff member and the Confidentiality Officer.

3. Legal analysis

Overall Europol manages well the verifications of the US DoT requests. The different actors complement each other and pay close attention to details.

The EDPS has identified good practices when Europol analyses the US requests. Europol takes into account other information than what is provided in the request to assess the necessity, such as the work experience of Europol staff, trends, statistics and intelligence provided for example in the TE-Sat. In addition, they receive regular training by the Designated Provider (DP) in order to keep staff members up to date as regards the message types and related data categories.

[1] Council Decision of 13 July 2010 on the Conclusion of the Agreement between the EU and USA on the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the Terrorist Finance Tracking Program, OJ L 195 of 27.7.2010, p.5.

The EDPS has the following recommendations to make:

Finding 1

The US DoT performs an annual large-scale audit of extracted data to identify the most relevant data in terms of message types and countries. The results of this exercise are taken into account for justification of the US requests for the countries and message types included. The analysis is not communicated to Europol but its results are reflected in the subsequent monthly requests.

Europol's role under Article 4 (4) is to verify whether the request complies with the requirements of paragraph 2, in particular the necessity of the data covered by the request in terms of countries and message types. At this stage, Europol only relies on the US claims that such assessment has been conducted without actually having access to this analysis.

Recommendation 1

Europol should ask the US DoT to provide the annual analysis to be in a position to actually check that the requests reflect the US DoT's necessity assessment in terms of countries and message types.

Finding 2

The inspected requests are voluminous. The amount of changes/updates from one request to the other is relatively limited but not highlighted. It is therefore not obvious to identify changes from one month to the other. This bears the risk that new critical information may be overlooked. Also, this makes it more difficult for Europol to verify compliance with Article 4.

Recommendation 2

Europol should ask the US DoT to make more visible the request's changes from one month to another. For instance, changes could be printed in bold or the US DoT could provide a version with track changes.

Finding 3

In line with the previous points, the verification forms justly contain the complete analysis of the requests. As information is duplicated from one request to the next, the most substantive elements lie in the changes.

Recommendation 3

Verification should highlight what has changed.

Finding 4

According to the TFTP Process Description "Art. 4 requests shall be archived for 5 years at the Confidentiality Desk in accordance with the provisions stipulated in the security manual. Thereafter, they shall be destroyed (…)". Europol has kept all requests and related verification forms since the inception of the TFTP agreement in 2010.

Recommendation 4

Europol should either destroy the requests and verification forms older than 5 years or they should justify and document the need for a continued retention of that information.

4. Information security analysis

After the interviews, it appears that information security has been implemented throughout the process (i.e. from getting the information from the US DoT, handling it and communicating the required information to the DP).

The EDPS has the following recommendations to make:

Finding 5

The TFTP requests are sent by the US DoT to Europol and to the DP (this is described in details in file n°2566-566; p.3 gives and overview of the process). It appears that, at no moment in the process, the information sent to the DP and to Europol is verified to ensure that Europol and the DP are working on an identical in substance document. Everything relies on trust in the US DoT integrity and their ability to work without making mistakes.

Recommendation 5

The process for transferring information from the US DoT to Europol and to the DP needs to be reviewed to provide assurance that Europol and the DP work on identical in substance documents.

Finding 6

According to p14 of file n°2566-566, the security measures implemented to ensure communication between Europol and the DP were determined following a Risk Assessment (RA). This RA was requested but not made available.

Recommendation 6

The EDPS requests the possibility to view this RA. The RA should be recent and there should be a process in place in Europol to review this RA and the security measures on a regular basis.

Finding 7

It is good practice to regularly review security needs to ensure their suitability in an ever-changing landscape. Thus, although the security classification of TFTP documents at the level of Secret EU/EU Secret (Europol) is derived from the security requirement of the US DoT, the security needs surrounding the TFTP documents should be reviewed taking into account the 9 years of experience in handling this information.

Recommendation 7

Europol should initiate discussions with the US DoT to verify if security needs are still suitable. A simplification of the process, the declassification of TFTP documents and the use of modern electronic means for the documents should be discussed.

Finding 8

[EU CLASSIFIED INFORMATION - REDACTED]

Recommendation 8

[EU CLASSIFIED INFORMATION - REDACTED]

Wojciech Rafał WIEWIÓROWSKI