VS - NUR FÜR DEN DIENSTGEBRAUCH

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[1] 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 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

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

VS - NUR FÜR DEN DIENSTGEBRAUCH

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.