

**Speaking Note for the Public Hearing before the LIBE
Committee of the European Parliament on the Future
of Europol, 10 April 2007**

Session III; The applicability of a general framework on
data protection

Sub session: *Europol framework for the transfer of data
towards third countries*

Contributor: Pelopidas Donos

Ladies and Gentlemen,

After Mr. Neumann has presented the general legal regime with regard to Europol's information exchange with Third Parties, I will focus on the practical implementation of the legal provisions. More specifically, I will provide you with an overview of the established procedures which Europol has in place in order to guarantee that the information workflow is controlled and in compliance with the legal requirements.

There are three general principles governing the exchange of information with Third Parties:

- There is one single point of input and output at Europol with regard to the exchange of information with Third Parties.
- Only evaluated data may be processed in Europol's systems and transmitted to Third Parties.
- There is an additional internal monitoring carried out by the Data Protection Office.

With regard to each of these principles:

Europol's Information Management Unit is the single point at Europol which manages the exchange of information with Third Parties.

If I may draw a parallel this Unit acts as a liaison unit on behalf of Third Parties between Europol (for example, the Serious Crime Units and the Analysis Work Files) and Member States in the daily management of information exchange. This regime allows Europol to safeguard the legality of the information exchange as well as to enrich

the use of data received from Third Parties by cross-checking data against Europol databases.

In practical terms this means that whenever information from a Third Party arrives at Europol, this Unit is responsible for controlling and initiating the input of data into the Information System.

The same Unit is also responsible for the output of the information. Every piece of information transmitted to a Third Party, regardless whether the data derives from an AWF or from the Information System, takes place via this single contact point.

As a result the information exchange can be better documented, monitored and audited.

Of course the responsibilities of the Unit go far beyond being a simple mail box, a point that brings me to the second important principle governing the information exchange which is the evaluation of the information.

Before being inserted in Europol's systems the data is scrutinised and evaluated by being crosschecked against specific criteria. The first check is the legality check and this aims to ensure that the information meets all legal requirements. For example a piece of information containing personal data not falling under the categories foreseen by the Convention will be rejected and the provider of the information will be informed. The legal check also includes the compliance with the confidentiality provisions of the cooperation agreement. Only after the legality check has been passed a second check regarding the operational value of the information will be made.

Following the same principle every transmission of information from Europol to a Third Party also undergoes an evaluation legality check. This check makes sure that for example information containing personal data will be never disclosed to a Third Party with which Europol has signed only a strategic cooperation agreement.

More specifically and with regard to the Analysis Work Files, the information is also crosschecked against the "opening order" before being inserted in the data base. As

you are aware the opening order is a kind of “contract” between Europol and the Joint Supervisory Body and describes in detail categories of data and categories of persons which can be processed in an AWF. Before taking a decision to insert the data Europol’s officials have to follow the established verification procedure.

The legal element of the verification process requires that the following five questions can be answered in the positive:

- Do you know who has provided the data?
- Have they given permission for it to be included in the AWF?
- Is it linked to a criminal offence within the scope of the Opening Order?
- Does it involve a category of person allowed by the AWF Opening Order?
- Does it involve a category of data allowed by the AWF Opening Order?

If the answer to any of these is “no” the data cannot be entered and should be returned to the contributing party.

In addition, verification includes an evaluation of the operational value of the data where the questions to be answered are the following:

- Is it recent operational information?
- Is it relevant to the current operational focus of the AWF?
- Is entering it into the AWF a good use of your current resources?

Whenever data contributions are refused, Europol explains the reasons for the refusal to the contributing party.

The third principle governing the information workflow is the additional control undertaken by the Data Protection Office. The Data Protection Officer by exercising his duties to ensure compliance with Europol's data protection obligations conducts regular checks in Europol's computerised systems. The results are documented, Europol's Director is then informed and the relevant logbooks are available to the JSB. Additionally to that the Data Protection Office advises the Information Management Unit on issues related to data protection.

Also in cases where a transmission of data to a Third Party has to take place on an exceptional basis, as it is described in Article 18 of the Convention amended by the so called Danish Protocol, Europol tries to have procedures in place guaranteeing that the decision taken is balanced and well documented. For that purpose and in the context of the preparations for the implementation of the protocols, a checklist has been prepared to be used by the Director whenever he decides to apply this exceptional clause. The objective is to facilitate the decision making process for the Director while providing the Management Board and the JSB with the necessary elements to help them evaluate the Director's decision to transmit data under the exceptional clause.

Ladies and gentlemen,

I hope that I managed to give you an overview of the strict procedures governing Europol's information exchange with Third Parties. As the Director has pointed out on several occasions Europol has a strong interest to have this kind of procedure in place, not only in order to comply with the legal requirements and protect the human rights,

but also in order to ensure and enhance the value and the quality of its information.

Thank you very much for your attention.

