



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 29 March 2012

8261/12

LIMITE

**JAI 205
COSI 13
ENFOPOL 86**

NOTE

From:	Commission services
To:	Standing Committee on operational co-operation on internal security (COSI)
No. prev. doc.:	7336/12 JAI 143 COSI 8 ENFOPOL 58
Subject:	Revision of Europol's legal basis

Delegations will find in annex a working paper from the Commission services with ideas for the revision of Europol's legal basis.

Contributing elements to these ideas, which are submitted to COSI members, are drawn from: the preliminary findings of the interim evaluation report by RAND, the first discussion in COSI in February¹, various stakeholder consultations and DG HOME internal discussions.

The overall goal is to improve Europol's operational efficiency and effectiveness and at the same time its accountability. No elements suggest its mandate should be broadened or reduced, but rather that an enhancement of its analytical and operational capabilities should be achieved. A number of objectives can serve to achieve this goal. In turn, several avenues could be pursued. It is on these that DG HOME seeks the views of COSI.

¹ 7336/12 JAI 143 COSI 8 ENFOPOL 58

Below are a number of objectives with ideas to achieve them:

1. Improving Europol's intelligence picture by enhancing the provision of information to Europol by MSs, in quality and quantity

- Introducing incentives to investigations to crime areas other than Euro counterfeiting.
- Checks and balances: to ensure MSs comply with their obligations vis-à-vis Europol, to establish the obligation of a periodic evaluation of the ENUs work/organisation and of that of national competent authorities (with a component of peer review). The details of the mechanism would have to be defined elsewhere, because the future Regulation will not contain a breakdown of the rules on which the evaluation criteria will be based.
- The obligation for MSs to provide Europol with relevant information in a timely fashion could also be extended from the ENUs to the national competent authorities.
- The obligation could also be strengthened by insisting on the need to contribute, in particular, in certain crime areas.

2. Ensuring that Europol has more effective contacts with MSs: reviewing the role of ENUs in order to give more space to national competent authorities to liaise with Europol

- The possibility of direct contacts with national competent authorities could be enshrined in the future Regulation, in order to streamline exchanges, especially on ongoing investigations. The ENUs would in any case need to be kept informed. Direct contacts with national competent authorities are already possible for Europol but are dependent on the will and decision of the individual MSs (Art. 8(2) of the ECD).
- The future Regulation could also prescribe that ENUs must have access to relevant national law enforcement data bases.

3. Facilitating access by Europol to private-sector held information

- To introduce provisions on information exchange with the private sector. Where relevant (need to know) the ENU would be informed. This could notably facilitate the work of the Cybercrime Centre.

4. Triggering investigative action at MS level: from Europol's analysis to national action: improving the follow-up given to Europol's findings

- To strengthen the provision that empowers Europol to request of MSs the initiation of a criminal investigation (Art. 7(1) ECD), by obliging them to supply a reasoned justification if they decide not to go ahead with the investigation within a given deadline.
- To strengthen Europol's obligation to inform Eurojust of a *notitia criminis*, in line with Art. 85 TFEU.

Ideally the two means should be cumulated: whilst Europol can address its request to ENUs or law enforcement competent authorities, Eurojust, based on the information supplied by Europol, should address the prosecution authorities. This construction is in line with the TFEU. This approach better articulates Europol and Eurojust's roles.

5. More flexibility in information management for better effectiveness: redesigning Europol's data management concept

- The future regulation could improve the information management system of Europol which currently defines in a prescriptive manner the data systems that Europol can use. This system has been identified as decreasing operational effectiveness of Europol. The Regulation would spell out strong data protection and data security rules. These rules would not possibly concern systems or data-bases, but instead they could apply to the specific type of information (information processed for cross-checking purposes, for strategic or general analysis purposes or for specific operational analysis purposes) leaving flexibility as to the most suitable IT architecture.

6. Rationalising Europol's means to exchange information with 3rd partners. Combining the legal requirement to align the legal basis with the Lisbon Treaty with the possibility to obtain and transmit data according to operational needs

- The system would have the following components:
 - a) The COM negotiates, on behalf of the EU an agreement with a 3rd state. It will require the technical support of Europol on aspects relating to law enforcement. This should be enshrined in the future Regulation.
 - b) The future Regulation should give Europol the mandate to conclude working arrangements with competent law enforcement authorities of 3rd states on the basis of an EU agreement, with the purpose of exchanging information other than personal data.
 - c) In the absence of an agreement, and in duly justified situations, Europol shall be entitled to exchange information on an ad hoc basis with law enforcement agencies in 3rd states for a limited duration and specific purpose, based on a prior authorisation of a data protection authority (ex.: JSB in cooperation with EDPS).
 - d) In the absence of an agreement, and in cases of urgency (imminent threat), on an exceptional basis, the Europol Director, having consulted the Chairman of the Management Board, can authorise the exchange of data (or only transmission or receipt) without prior authorisation but must inform the data protection authority mentioned above.

7. Strengthening the external data protection supervisory authority
