EUROPEAN
COMMISSION

Brussels, 27.3.2013
SWD(2013) 99 final

Part 1

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT on adapting the European police Office's legal framework with the Lisbon Treaty

Accompanying the document

Proposal for a EUROPEAN PARLIAMENT and COUNCIL REGULATION

ON THE EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION AND TRAINING (EUROPOL) AND REPEALING COUNCIL DECISIONS 2009/371/JHA AND 2005/681/JHA

{COM(2013) 173 final}
{SWD(2013) 98 final}
{SWD(2013) 100 final}

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT on adapting the European police Office's legal framework with the Lisbon Treaty

Accompanying the document

Proposal for a EUROPEAN PARLIAMENT and COUNCIL REGULATION

ON THE EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION AND TRAINING (EUROPOL) AND REPEALING COUNCIL DECISIONS 2009/371/JHA AND 2005/681/JHA

Article 88 of the TFEU provides for a new legal basis for Europol (regulation) and for the scrutiny of its activities by the European Parliament together with national parliaments.

In addition, the Stockholm Program[1] has stressed that organised crime has become more globalised, that the fight against it requires, inter alia, systematic exchange of information and called for Europol to become a "hub for information exchange between the law enforcement agencies of the Member States, a service provider and a platform for law enforcement services[2]".

An evaluation study confirms that Europol adds value to the security of European citizens and has a robust data protection regime. Nevertheless, it identified a number of areas where improvements are needed to allow Europol to meet the goals of the Stockholm Programme.

This reform is intended to form a part of a wider package which includes a proposal to merge the European Police College or 'CEPOL' with Europol and to implement a European Law Enforcement Training Scheme (LETS) for law enforcement officials.

Finally, by reforming Europol the Commission is committed to apply the governance standards agreed together with the European Parliament and Council in July 2012 in the Common Approach on EU decentralised agencies[3].

In preparing this impact assessment, the Commission has consulted all major stakeholder groups.

1. PROBLEM DEFINITION

Large scale criminal and terrorist networks pose a significant threat to the internal security of the EU. National law enforcement services can no longer work in isolation and need to cooperate.

---

1 The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens, OJ C 115, 4.5.2010, p. 1–38

2 The European Council also invited the Commission to "examine how it could be ensured that Europol receives information from Member States law enforcement authorities so that the Member States can make full use of Europol capacities".

3 http://europa.eu/agencies/documents/joint_statement_and_common_approach_2012_en.pdf

The creation of a common space without internal borders, and the further integration of the European Union have greatly benefited the free movement of EU citizens; they had to be accompanied by a reinforcement of security measures to tackle cross-border crime. The establishment of Europol – the EU agency designed to help law enforcement authorities of the EU better cooperate with one another – is instrumental in this regard.

Europol provides assistance to national police forces, notably by facilitating the **sharing of criminal information**. It produces **operational analyses** which help law enforcement services in transnational investigations. It offers **operational assistance** (expertise) in support of cross-border investigations or coordinates them; it gives financial support for euro-counterfeiting investigations. It also provides **strategic analysis in the form of threat assessments.** Europol has **neither autonomous investigative capabilities nor coercive powers.**

1.1. Description of the problem

The Commission has identified several shortcomings that prevent Europol from becoming a hub of information exchange between law enforcement officers in the Member States.

PROBLEM 1

1.1.1. Member States do not provide Europol with all the necessary information to fight serious cross-border crime

The EU has placed initiatives - both legislative and financial - to promote information exchange at the heart of its policies in the area of Home Affairs. Europol depends predominantly on the Member States for collecting data and intelligence. The Council Decision requires Member States **to supply Europol with data** that falls within its mandate.

However, Member States do not provide Europol all necessary information to fight crime or do not do it in a timely manner. There are also important discrepancies between the Member States in the provision of information. Various statistics confirm this.

Underlying **drivers are**:

- **Lack of precision of existing legal provisions:** The obligation of Member States to provide data is not formulated in an explicit way, thus leaving room for contradictory interpretations and for doubts on the type, level of detail and extent of information Member States should send to Europol. Some Members States do not even recognize the existence of an obligation.

- **Sociological and cultural drivers: Low awareness, lack of knowledge, a policing culture** which encourages law enforcement officers to be **cautious about information sharing**.

- **Organisational drivers:** some organisational factors impact upon the performance and effectiveness of the Europol National Units (ENUs), set-up in each Member State to be the contact point for Europol.

Reluctance to transmit information prevents Europol from identifying links with crime phenomena in other countries and from creating an accurate criminal intelligence picture throughout the EU, which could allow it to coordinate investigative action by Member States.

As a result, as Member States do not see sufficient added value in Europol's findings, they are less motivated to supply information to the agency.

PROBLEM 2

1.1.2. Constraints on data processing

Europol manages several databases to assist Member States in preventing and combatting serious cross-border crime and terrorism. The Europol Council Decision pre-defines strictly these databases and attaches to them different purposes, different rules on who could access them and specific provisions on data protection and security.

The Europol Information System (the EIS) is a reference database used for cross-matching purposes. Analysis Work Files are databases for analytical operational purposes and for assisting live investigations. They combine hard data used for identification with intelligence. One AWF concerns serious and organised crime (the AWF SOC), the other terrorism (the AWF CT).

The Member State which provides the data is its owner. It decides the purpose for which it is transmitted to Europol (for simple reference purposes in the EIS, or for specific analysis purposes in one of the several AWFs); in addition, it can decide who can access them and what use can be made of them (“owner principle”).

Only mere cross-matching is possible across the databases (detecting if the same data entity is in another database). Linking of information across different databases is not permitted for a Europol analyst, unless he receives authorisation from all those who provided these data to database to which he has no access. In practice it takes from a few weeks to a few months.

Only linking of data entities (detecting relations between the data) allows an analyst to assess relevance of information for the analysis and gives a meaning to information about criminal or terrorist organisations, e.g. a hypothesis on the role of the individual perpetrator in the hierarchy of a criminal group involved in both serious crime and terrorism (e.g. smuggling drugs or weapons to sponsor terrorist activities). Without linking there is no criminal analysis.

All this prevents an efficient analysis and delays identification of trends and patterns in criminal activities. Europol cannot produce intelligence reports on criminals, terrorists and their links, which can be necessary for Member States' investigations.

In addition, data sent by a Member State can be intended both for sharing in the EIS and for analysis in the AWFs. The technical separation implies that the data must be stored at least twice (or three times) with duplicated obligations for the data owner as well as for Europol to maintain (update, delete) the data, and risks of introducing differences between originally equal data sets.

1.2. THE BASELINE SCENARIO

Establishing Europol's scrutiny by the European Parliament and national parliaments would enhance its accountability but would not have impact on Europol's becoming information hub for law enforcement authorities. The level of information supply should continue to grow, but discrepancies among Member States would persist. On data management, storing data in databases technically separated will continue to limit Europol’s capacity to deliver

comprehensive analytical reports to Member States, especially on the links between organised crime groups and terrorist networks. Europol's analysts would not be able to link information on organised crime and terrorist networks (stored in different AWFs and the EIS). Delays in identifying trends and patters in this context will persist. A possibility of multiple storage of data in two or three places would continue.

2. POLICY OBJECTIVES

General objective of Europol's reform: to increase security of the EU by making Europol a hub for information exchange between law enforcement authorities in the Member States so as to better support them in preventing and combatting serious cross-border crime and terrorism.

Specific and operational objectives

1. To increase provision of information to Europol by Member States

(a) To increase volume and quality of information provided to Europol by Member States

(b) To reduce discrepancies in level of information provision by Member States

2. To establish a data processing environment that will allow Europol's analysts to fully assist Member States in preventing and combating serious cross-border crime and terrorism

(c) To ensure that Europol's analysts could link and make analyses of all relevant pieces of data;

(d) To reduce delays in identifying trends and patterns;

(e) To reduce multiple storage of data.

3. POLICY OPTIONS

3.1. Option 1: Baseline scenario/"Pure lisbonisation"

To garner more contributions from Member States Europol, in cooperation with CEPOL and the Commission, will continue "soft measures" - awareness raising in the form of road shows, training promotion of good practices of ENUs.

Analysis building will rely on separated databases with limited possibilities of linking and analysing data scattered around different databases.

3.2. Option 2: Making further legislative amendments through the Europol regulation

A. Provision of information from Member States

A.1 Strengthening obligations and introducing incentives

The regulation will provide for:

- continued awareness raising;
- the clarification of the legal provision on obligation to provide data: Member States would be obliged to share all data falling under Europol's mandate and in particular

those actually exchanged with another Member State. To achieve prioritisation, the obligation would be focused on information on crime identified as EU priorities in the EU Policy Cycle on organised and serious international crime;

- monitoring how Member States respect the obligation: Europol will submit an annual report to Parliament and Council on information provision by individual Member States and performance of ENUs;
- financial incentives to Member States – the Regulation would extend financial assistance to support Member States' investigations in crime areas other than Euro counterfeiting.

A.2. Giving Europol access to law enforcement databases of Member States

Through access to national law enforcement databases on a "hit-no-hit" basis, Europol would detect that a Member State is in possession of relevant information. Then, following a "hit", Europol could request this information. Member States would keep control over data as their authorisation for the transfer is necessary.

This system would require a new IT architecture: 1) a forwarding system which would send queries to Member State and assemble the replies on hits, 2) investments of Member States to reorganise their databases to separate data falling within Europol's mandate or setting up a forwarding database, as well as to provide appropriate IT connections.

B. Data management

B.1. Merging the existing two AWFs into one

Under this option, the two existing AWFs are merged into one and the EIS remains separated.

B.2. New processing environment

Europol regulation will no longer be "database-oriented". It would lay down procedural safeguards to implement data protection principles with particular emphasis on ‘privacy by design’ and full transparency towards the Data Protection Officer of Europol and supervisory authorities. Bound by "Privacy by design", Europol would take all the data protection requirements into account from the outset when designing specifications and architecture of communication systems and technologies.

There are several technical solutions to achieve this aim. Whatever is pursued:

- Data protection safeguards will be attached to the piece and type of data rather than to a predefined data base;
- To ensure purpose limitation the data supplier would determine from the outset the purpose of processing operation for which data are shared with Europol (cross-checking, operational analysis, general analysis);
- All information would be fully visible to Europol's analysts as long as it is necessary for his tasks. Nevertheless, Europol's partners will still be entitled to impose restrictions to access and use by others.

4. ANALYSIS OF IMPACT

4.1. Option 1: Baseline Scenario/"pure lisbonisation"

Increasing security in the EU (0): Europol will continue to have a fragmented picture of the EU-criminality. Member States would not be sufficiently assisted.

Protection of personal data (0): no impact on protection of personal data, no positive indirect impact on the right to life.

Costs (0): no new costs compared to the status quo

Option 2: Making further legislative amendments to the Europol regulation

4.1.1. Impacts of the options under policy option A

4.1.1.1. Strengthening obligations and introducing additional incentives (A1)

Increasing security in the EU (+++): positive impact on shortcomings and increase of both volume and quality of information sent by Member States.

Focusing on the goals of the EU Policy Cycle and sharing information that they exchange bilaterally would result in a higher in-flow of data to Europol on the most important threats.

Monitoring the performance of ENUs and the provision of information by each Member State would create peer pressure. This would encourage good practices, including on efficient organisation of ENUs, awareness raising and strengthening cooperation between ENUs and national law enforcement.

If cross-border investigations received financial support, this would encourage Member States to involve Europol more.

Several successes in counterfeiting demonstrate it.

Protection of personal data (0): no impact compared to the baseline.

Costs (--):

For the EU budget:

- the costs of 6 staff to handle a higher amount of data provided
- Financial support for Member States' investigations beyond Euro-counterfeiting amounting to 800.000 € yearly (offset by cutting some activities of the Management Board of Europol).

For national budgets:

- no material costs.
- Costs to Member States for one-time training of law enforcement officers dealing with serious cross-border crime: EUR 600 000 or EUR 3m or EUR 6m
- On a case-by-case basis, possible reorganisation of ENUs.

Benefits: Increase in effectiveness of the fight against serious cross-border crime-millions of EUR in 2015-2020

4.1.1.2. Giving Europol access to law enforcement databases of Member States (A2)

Increasing security in the EU (+++): would overcome the lack of knowledge, ineffective ENUs or low awareness of Member States. Member States will retain control over data as they would authorise the transfer.

A greater amount of more relevant information will reach Europol, which would be able to offer better quality products to Member States.

Protection of personal data (0) None. Access would be on a hit-no-hit basis. To receive the content of the information Europol would need to request the Member State. Before transmission the Member State would ensure all data protection safeguards.

Costs (---):

For the EU budget:

(1) EUR 1,78 m one off investment and

(2) EUR 1,46 m of yearly recurring investments.

Costs for the MS budgets:

- EUR 660,000 one-time investments for the adaptation of their IT systems and connection to the forwarding system;
- Recurring investments of EUR 1,2 m annually;
- On a case-by-case basis possible costs of additional 1-2 staff.

4.1.2. Impacts of policy option B

4.1.2.1. Merging of two AWFs into one (B1)

Increasing security in the EU (++): It would potentially entail a faster identification of trends, patterns and links between criminal groups involved also in terrorism.

Thanks to broadening of scope of an AWF to cover both serious organised crime and terrorism, Europol's analysts would be able to visualise all links between information provided to the merged AWF. Linking the data from EIS system with those in the AWF will still not be possible. Multiple storage of data will persist.

Protection of personal data (0): There will be no impact on protection of personal data compared to the baseline as this option is a mere extension of the current system.

Costs (0): It would entail minimal costs as the two AWFs to be merged are supported by the same technological solutions. They could be borne by Europol's IT budget. The necessary investments and consultancy work were done by preparing the recent merger of 23 AWFs into two, therefore its results could be reused.

4.1.2.2 New processing environment (B2)

Increasing security in the EU (+++): Europol analysts would be able to link and analyse all data that are necessary for them. This would allow Europol to build a bridge between all aspects of the fight against organized crime and terrorism. Within a single processing environment Europol would be able to better identify, analyse and define the structures

linking organized crime groups and terrorist networks, for instance through the financial trails.

Impacts on the protection of personal data (0): At least the same level of data protection as in the baseline would apply.

Impact on Costs (0): This option would not entail any immediate additional expenditure compared to the baseline.

5. PREFERRED POLICY OPTION

The preferred policy options would be Option 2 (further legislative changes) consisting of Option A1 and B2.

- Thanks to incentives and the strengthening of the obligation to provide information, Member States would have more clarity and would become more motivated to send data.
- The new rules on data management would allow Europol's analysts to have access to all information they needs to know, to determine links between information and to identify trends and patterns. Europol would offer more relevant and up-to-date products to assist Member States. There will be no multiple storage of data.

As to the costs:

- Financial support offered by Europol to Member States' investigations would require 800.000 € per annum, to reach a critical mass of funding. These funds will be found by reprioritising Europol's budget.
- The total staff that Europol needs to implement this reform is 6 FTE that is needed to handle a higher inflow of information from Member States. Three staff will be redeployed; three others would need to be employed. The total staff costs would then reach EUR 1.77 m over the period from 2015 to 2020. However, approximately two thirds of these costs will be offset by the savings resulting from the merger with CEPOL.
- There will be no immediate costs in view of new data management rules.