



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 14 June 2013

10988/13

**Interinstitutional File:
2013/0091 (COD)**

**ENFOPOL 189
CODEC 1474**

NOTE

From: General Secretariat
To: Law Enforcement Working Party
No. prev. doc.: 8229/13 ENFOPOL 98 CODEC 746
Subject: Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol)
- Opinion of the Joint Supervisory Body of Europol (Opinion 13/31)

Delegations will find attached the Opinion of the Joint Supervisory Body of Europol (Opinion 13/31) with respect to the proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol).

Opinion of the Joint Supervisory Body of Europol

(Opinion 13/31)

**with respect to the proposal for a Regulation of the European Parliament and of the Council
on the European Union Agency for Law Enforcement Cooperation and Training (Europol)**

Brussels: 10 June 2013

Management summary

Europol's existing robust data protection regime, safeguarded by strict, tailor-made rules and effective supervision arrangements, is the benchmark for assessing the proposed new further legal basis for Europol.

The key assessment of the Joint Supervisory Body of Europol (JSB) is that the Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol)¹ (hereinafter the regulation) would result in a much weaker Europol data protection regime. The assessment of the JSB is in line with the views of the European national data protection authorities, who clarified their views at the Conference of European Data Protection Authorities, Lisbon 16-17 May 2013, by adopting a resolution on ensuring an adequate level of data protection at Europol.

Europol's legal basis must contain specific provisions for data processing and responsibilities in relation to each task and each data processing facility. The regulation falls short of this.

Considering the ongoing review of the data protection rules - including a proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - it would have been preferable to wait for the outcome of this process in order to allow reference to the basic provisions in the resulting data protection package.

This opinion discusses the data protection issues in the regulation which would put Europol most at risk and which could negatively impact the safeguarding of individuals' rights. Where possible, solutions or amends are suggested with a view to improving the regulation.

The JSB will publish its assessment of the Articles of the regulation relevant to data protection in due course.

The main issues further discussed in this opinion include:

¹ COM(2013) 173 final

Europol's role and responsibilities, which will be extended under the regulation, include a coordinating role in investigations. These new roles will impact the organisation of Europol's work and the relation with the Member States, particularly concerning data exchange and setting priorities and purposes for data processing. The regulation does not set out how the different responsibilities involved would be distributed between Europol and the participating Member States.

Changes to the crimes for which Europol is competent. The Commission appears to have departed from the definition of serious crime that has been practice for the last decade. Ever since the introduction of the European Arrest Warrant, a serious crime was defined in the same way, taking due account of the national legislation of the Member States. It is unclear why this well-known definition has not been maintained. Instead, the regulation introduces the criterion “forms of crime which affect a common interest covered by a Union policy”.

Europol's tasks, including the recent and planned future developments with the Secure Information Network Application (SIENA), which puts Europol in a service-provider role and encompasses exchanges of information in various directions between Europol, the Member States and Third parties. This role and some of these forms of communication have no legal basis in the regulation.

Changes to the processing environment, even though the changes in the approach to crime analysis from the start of Europol to the present date has never been hampered by the existing legal structure of analytical work files or the IT systems. In view of the current practice and experiences, the arguments presented for changing the data processing structures are unconvincing. The choice of the purpose of processing and the necessary data files to achieve Europol's objectives shouldn't be defined by IT structures. Principles of data protection such as necessity and purpose limitation should not be made dependant on a choice of IT structure. A clear set of provisions dealing with the responsibilities - in a flexible structure - is required to fulfil Europol's tasks and to ensure adequate data protection safeguards. The JSB stresses that flexibility depends on the possibilities - and resources - of Europol to comply with Member States' requests for support. Additionally, the Europol Council Decision already introduced a provision allowing Europol to act more flexibly and create new systems when necessary; Europol has never used this possibility, which could indicate that the present system is flexible enough.

Controllability, including the welcome introduction of parliamentary scrutiny, but raising the issue of potentially weakened control by the data providers - by and large the Member States.

Data protection supervision, and the need to maintain the strong involvement of the national DPAs in the supervision of Europol, while modernising the institutional arrangement. **The involvement of the national DPAs is essential because the vast majority of data collected and processed by Europol originates from the Member States and is sent back to the Member States.**

The specific role of Europol requires effective joint supervision including the national DPAs as well as the EDPS. **The JSB does not support the idea of the Commission to make the EDPS solely responsible for the supervision of Europol.** The extensive national experience of how to deal with law enforcement information is required. **The JSB proposes the creation of an independent and effective joint supervision structure with equal participation of each national DPA and the EDPS.**

1. Introduction

On 27 March 2013, the Commission presented the regulation, which will repeal Decision 2009/371/JHA (Europol Council Decision) and Decision 2005/681/JHA (CEPOL Council Decision).

As the data protection supervisor of Europol, the JSB sees it as its task to assess the regulation. The following opinion is based on the extensive experience² the JSB has with the daily work and data processing activities of Europol. In view of the JSB's composition,³ this opinion also reflects the national experiences with data processing at Europol.

As JSB underlined in its first activity report, (1998-2002) *"data protection cannot exist merely as an abstract concept: Europol must apply the rules laid down in the Europol Convention and the organisation should be conversant with the key principles of data protection."*

The high level of data protection provisions embedded in the Europol Convention and Decision 2009/371/JHA have proven their value. Europol implemented these rules in their organisation and became a benchmark for the balance between law enforcement and data protection. The regulation should at least maintain that high level.

This opinion is divided into the following chapters:

2. Level of data protection
3. Europol's role and responsibilities
4. Europol's tasks
5. Choice of processing environment
6. Controllability
7. Data protection supervision - controlling Europol's data processing
8. Conclusion

An opinion containing an assessment of all relevant articles will be presented in due course.

² The JSB started its work in October 1998

³ The JSB is composed of representatives of the national data protection authorities

2. Level of data protection

The JSB has highlighted frequently that the existing Europol data protection regime should be categorised as a strong and robust one. This opinion was based on the strict and tailor made data protection rules applicable to Europol's activities, the manner in which supervision is executed in practice and the close cooperation between the JSB and Europol to implement data protection in the daily work.⁴ A crucial element in this assessment is that Europol's legal basis contains specific provisions for data processing and responsibilities in relation to the different tasks and subsequent data processing facilities of Europol. In view of Europol's task and the close relation with national law enforcement activities this has proven to be vital for a sound balance between the interests of data protection and law enforcement.

The regulation replaces this by defining a set of general principles and relies on a privacy-by-design approach⁵. There are no rules applicable to specific data processing activities to be chosen by Europol that guarantee tailor made implementation of the general principles. The term “privacy by design” is not sufficiently specified as to content.

The JSB assesses the level of data protection introduced by the regulation, also in view of the new competences of Europol as a clear retrograde step compared to the existing level of data protection set out in the Europol Council Decision. This is also the assessment of all national data protection authorities.⁶

⁴ See also Rand report on Evaluation of the implementation of the Europol Council Decision and of Europol's Activities Chapter 7.7.

⁵ Explanatory Memorandum, page 7

⁶ Resolution of the Conference of European Data Protection Authorities, Lisbon 16-17 May 2013, on ensuring an adequate level of data protection at Europol.

A further remark concerns the embedding of the Europol data protection provisions in a broader perspective. Both the Europol Council Decision and the regulation apply the principles of data protection as defined in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and in the Recommendation No R(87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987.⁷ When the Commission presented the regulation, negotiations on the data protection reform package were, and still are, ongoing. Part of that package is a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. This directive, although not applicable to the work of Europol, is an important data protection instrument as it defines the data protection principles at national level in the area of law enforcement. In view of the relation between the activities of Europol and the national law enforcement authorities, **a close alignment between the data protection principles and provisions applicable to Europol and the draft directive should be ensured in the regulation.** Close alignment is also important for the supervisory tasks of the national data protection supervisors responsible for data processing on national level and involved in the supervision of Europol.

Since the review of the data protection legislation is ongoing it would have been preferable to wait for the outcome of the revision process in order to be able to refer to the basic provisions in the data protection regulation and directive.

3. Europol's role and responsibilities

The Treaty on European Union⁸ stimulated Member States' cooperation through Europol. More specifically, the Treaty obliged the Council to promote cooperation by enabling Europol to facilitate and support the preparation, and to encourage the coordination and carrying out of specific investigative actions by competent authorities of the Member States.

⁷ Article 27 Europol Council Decision and Chapter 4 of the Explanatory Memorandum

⁸ Article 30 Treaty on European Union, OJ C 325, 24.12.2002

Since its start, Europol's activities were always guided by Member States' requests for support and joint activities, resulting in sharing information and analysing data. Europol facilitated these joint activities by offering a platform for cooperation, an IT structure for sharing information (the Europol Information System, analytical work files, the index function and a messaging system) and specialists knowledge on crime analysis. There is a consensus among the Member States that the unique service Europol provides represents an added value to their everyday work of combating terrorism and serious crimes by Europol's network of Liaison Officers, the specially designed platforms Europol provides for information exchange and Europol's criminal intelligence analysis.

Lessons learnt from the practical implementation of the legal basis of Europol combined with a shifting world of how terrorism and crime manifests itself has led to several changes in policies on how to combat crime and changes regarding the data processing possibilities of Europol.⁹ The Europol Convention was changed four times and was later replaced by the Europol Council Decision. This last change also introduced new possibilities for Europol to process data and offered flexibility for Europol to adapt data processing to new challenges and developments by introducing the possibility to set up new information systems other than the ones defined in the Europol Council Decision.¹⁰

With the Treaty of Lisbon two new elements in the role of Europol were introduced.

Article 88(1)(b) of the Treaty on the Functioning of the European Union (TFEU) specifically mentions that Europol may have a role in coordinating, organising and implementing investigative and operational actions carried out jointly with the Member States' competent authorities or in the context of joint investigation teams; though any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member States or States whose territory is concerned.¹¹ **Europol's role - when compared with the situation before the Lisbon Treaty - is extended to include a coordinating role in investigations. This new role will have an impact on organising Europol's work and the relation with the Member States.** This is especially the situation concerning the data exchange and setting the priorities and purposes for data processing. **The regulation does not provide for rules on how the different responsibilities involved in such coordinated actions are distributed between Europol and the participating Member States.**

⁹ E.g. in 2002, Europol was given the possibility to request Member States to initiate criminal investigations.

¹⁰ Article 10(2) of the Europol Council Decision

¹¹ See Article 88(3) TFEU

The crimes for which Europol is competent also change. Apart from the crimes for which Europol is competent under the Europol Council Decision, its competence is extended to crimes which affect a common interest covered by a Union policy. The JSB assumes that this refers to the priorities set by the Council of the European Union based on a threat assessment of serious and organised crime. However, **the list of crimes referred to in Article 3(1) of the regulation includes some which are difficult to relate to a Union policy (murder, grievous bodily injury).**

The Commission also decided to depart from the definition of serious crime that has been practice for the last decade. Since the introduction of the European Arrest Warrant, a serious crime was defined in the same way, taking due account of the national legislation of the Member States. It is unclear why this well-known definition has not been maintained. Instead, the Europol Regulation now introduces the criterion “forms of crime which affect a common interest covered by a Union policy.” Even though the list of crimes in the Annex is similar for the Europol Regulation, the Europol Council Decision and the European Arrest Warrant, this change of approach needs to be well motivated (and currently it is not).

Another development is the strive to let Europol become a hub for information exchange between the law enforcement authorities of the Member States and a service provider.¹² Although a practical explanation of the consequences of this policy is lacking, the regulation clearly aims to place Europol as a unique centre where all law enforcement information falling within Europol's competence must be processed. The regulation aims to achieve that by strengthening the obligation for Member States to provide Europol with relevant data.¹³ The JSB notes that the only new obligation introduced in the regulation is Article 7(5)(a), stating that Member States shall provide Europol with a copy of bilateral or multilateral exchanges with another Member State or Member States in so far as the exchange refers to crime falling under Europol's objective. It is not clear whether this general obligation will lead to a situation where Member States must transmit all relevant data in ongoing investigations in which Europol's support is not requested but that might be relevant to Europol's competence. Practice has demonstrated that operational reasons sometimes prevent Member States from doing so. It is also not clear what is to be considered as "relevant data."

¹² Stockholm Programme OJ C 115, 4.5.2010

¹³ Explanatory Memorandum, page 6

It seems that the regulation - making Europol the hub for information - apparently intends that all information as referred to in Annex 2 to the regulation must be transmitted to Europol. As the regulation does not link the obligation to send data to Europol to a specific purpose and data processing system, this obligation will be the basis for creating one data processing system containing all law enforcement information Member States are obliged to send to Europol: the creation of one big Europol Information System, similar to the one defined in the Europol Council Decision but far more extensive in content.

From a data protection perspective the creation of such a system, or even the possibility of that, should be conditional on an impact assessment and in view of the impact of such a system specific data protection guarantees must be laid down in the regulation.

An understanding of Europol's role is important for the allocation of responsibilities for data processing in the area of law enforcement. The collection of data through operational actions and its subsequent use in investigations has been and will remain a national competence subject to national judicial scrutiny. When defining Europol's role in law enforcement activities and its impact on national law enforcement and judicial proceedings, **it is important that Europol's responsibilities for operational actions and data processing are complementary to national responsibilities and do not replace them.** As the regulation aims to grant Europol new responsibilities so that it may provide more comprehensive support for law enforcement authorities in the Member States,¹⁴ including a coordinating role, it will be important to explore the extent to which these new responsibilities replace or complement national responsibilities. A basic rule is that Europol is only allowed to process data when Member States are allowed to process these data. It is also unclear whether the allocated responsibilities for data processing by Europol in the regulation are compliant with this complementary character. **This subject will be further assessed in the further opinion on the articles of the regulation.**

The regulation also fuses Europol and Cefpol into one organisation. Europol will also be responsible for a coherent European training policy. This opinion will only refer to this new task of Europol when relevant in the framework of this opinion.

¹⁴ Explanatory Memorandum, page 5

4. Europol's tasks

In this Chapter the JSB will highlight some principal aspects.

As in the Europol Council Decision, the regulation defines Europol's tasks. Article 4 of the regulation provides for a list of tasks, some of them the same as in the Europol Council Decision, some of them new. The new tasks are related to the new task of Europol - the coordinating role - some introduce a task to transmit information to Union bodies or EU crisis management structures.

The new coordination task is further defined in Article 4(1)(c). An interesting aspect is that Europol's task also involves the implementation of investigative and operational action. Referring to what is already stated in Chapter 3 on Europol's responsibilities, it should be made clear in the regulation to what extent the task to implement investigative and operational actions creates a responsibility for these actions and the subsequent data collection and what would be the consequences for national judicial scrutiny. In particular, the responsibility for lawful processing is directly related to the responsibilities linked to this task.

Concerning Article 4(1)(j-k), the JSB wonders why these obligations to transmit data are listed in Article 4 and not introduced in Chapter VI of the regulation dealing with relation with partners.

The tasks as described in Article 4 are directly linked to the objectives of Europol. Since these objectives regard the actions of law enforcement authorities of Member States introducing tasks not linked to these authorities is not justified.

In particular, the provision allowing Europol to provide information and support to EU crisis management structures needs special attention since it does not comply with the common provision of Article 29: those structures are not to be considered Union bodies or international organisations. And as practice has demonstrated, personal data are transmitted by these management structures to Third states. Presenting these obligations as a separate task without any specific provision regulating the data protection safeguards is not in compliance with the basic principles for data protection especially concerning data transfer to Third states. **The tasks as defined in Article 4(1)(j and k) should be deleted and further regulated in Chapter VI.**

Some years ago, Europol introduced a messaging system for the exchange of information within Europol and between Europol and Member States: the Secure Information Exchange Network Application (SIENA). The JSB has been involved from the beginning of the development of SIENA.

SIENA has become an important tool for data exchange in the law enforcement area and is used by an increasing group of authorities. SIENA is not only used for communication within Europol and to and from Europol, it is also a messaging system between law enforcement authorities in cases where Europol is not involved (e.g. exchange not related to crime for which Europol is competent) or addressed to. Apart from the authorities in the Member States, most Third parties having a strategic or operational agreement with Europol are directly connected to SIENA. A continuous process of developing the functionalities of SIENA takes place. One of the consequences of the use of SIENA is the central processing of all SIENA messages at Europol including messages exchanged between law enforcement authorities from Member States and Third parties not related to Europol crimes or not directed to Europol. It is clear that the services offered by Europol to law enforcement authorities to use SIENA puts Europol in a service provider role, but another service provider than referred to in the page 2 of the Explanatory Memorandum. Europol processes data on behalf of another party and has no access to those data and no influence on the use of those data. These different roles of Europol may be compared with the different roles of a controller and processor as defined in Directive 95/46/EC.¹⁵ The regulation must provide for a legal basis for such a role of Europol, the use of SIENA as the messaging system for law enforcement authorities of Member States and Third parties, the data protection safeguards and the allocation of responsibilities for the content of the messages. **The necessary legal provisions in the regulation for SIENA should clearly establish a legal basis for the messaging service Europol provides and for any possible future use of a messaging system by Member States and Third parties. Especially the use of SIENA between Third parties should be explored and regulated.**

¹⁵ See also Article 4 (5-6) of the draft Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data and, Article 3 (6-7) of the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement.

One of the issues not addressed in the current proposals is the fact that Europol has been given a role under an international agreement which did not completely fall within its mandate or task description (TFTP Agreement). No provisions are foreseen to clarify Europol's role under the agreement and/or to ensure that future additional tasks under international agreements can be executed without problems with the legal basis. As stated above, additional tasks for Europol should be linked to the objectives of Europol.

5 Choice of processing environment

The results of the assessment of the policy objective on a data processing environment has according to the Explanatory Memorandum¹⁶ led to the choice for a new processing environment setting up procedural safeguards to implement data protection. The regulation does not provide descriptions of the type of data processing systems and the connected obligations and responsibilities. According to the Explanatory Memorandum, the agency's processing architecture is redesigned to better establish links between data in its possession. It enables Europol to adapt its IT architecture to future challenges and the need of law enforcement authorities. Advantages mentioned are to allow Europol to link and make analysis of relevant data, reduce delays in identifying trends and patterns and reduce multiple (duplicated) storage. Europol would be able to quickly identify trends and patterns across all criminal areas.¹⁷

As a first remark, the JSB notes that the introduction of a new analytical work concept in May 2012 with one file on organised crime and one on counter terrorism, each containing focal points and target groups, was introduced for exactly the same reasons as referred to in the Explanatory Memorandum for not having such defined structured files.

In view of the current practice and experiences, the arguments presented for changing the data processing structures are unconvincing.

¹⁶ Page 5 of the Explanatory Memorandum

¹⁷ Page 7 of the Explanatory Memorandum

The JSB doubts whether the choice of an IT structure may be used as an argument.¹⁸ **The choice of the purpose of data processing and the necessary data files to achieve Europol's objectives shouldn't be defined by IT structures. Principles of data protection such as necessity and purpose limitation should not be made dependant on the choice of an IT structure.** It is in fact the other way around. The JSB's experience in the past decade has shown that the question of whether Europol could adapt its organisation and data processing to new challenges and needs of law enforcement authorities is not necessarily linked to a choice of IT structure. The changes in the approach to crime analysis from the start of Europol to now was never hampered by the existing legal structure of analytical work files or used IT system. The changes in strategy from subject related analysis to a hub-based approach and later on the merging of several work files into two main files was possible within the same legal structure and using various IT structures. This does not mean that no improvements in flexibility can be made but it raises serious doubts about whether no provision at all - as now proposed - would be the answer. The JSB highlights that **flexibility depends on the possibilities of Europol to comply with various requests for support of Member States and the necessary allocation of sufficient resources.** Another aspect of flexibility is the question of Member States' abilities to adjust their structures to what is proposed by Europol when dealing with specific forms of crime, or a strategic change in dealing with multi-commodity criminal organisations. From another perspective, a question can also be raised as to whether flexibility also relates to Europol adjusting its data processing structures to Member States' needs. This is very important in view of the implementation of data protection responsibilities and the rights and obligations of the Member States and possibly Third parties in specific data processing activities. The Europol Decision and Council Decision 2009/936/JHA adopting the implementing rules for Europol analysis work files provide for clear rules for deciding on the participation of Member States and Third parties to specific analysing activities and the subsequent responsibilities. The regulation does not provide for instruments dealing with these issues.

The motivation presented in the Explanatory Memorandum does not justify the choice to have no provisions at all, other than stating that data processing should be introduced by privacy by design. **A clear set of provisions dealing with the responsibilities - in a flexible structure - for fulfilling Europol's tasks and for ensuring adequate data protection safeguards is required.**

¹⁸ Consideration 20, page 15 of the regulation

The JSB furthermore reiterates that the Europol Council Decision already introduced a provision allowing Europol to act flexibly and create new systems when necessary. Europol has never used this possibility, which could be seen as a signal that the present system is in fact flexible enough.

6. Controllability

The introduction of parliamentary scrutiny of law enforcement - a major step forward - is very much welcomed by the JSB. Cooperation between the European parliament and national parliaments for this scrutiny has been under discussion for over a decade and it is positive that the discussion can now be closed. The JSB only stresses the need to ensure the interinstitutional agreements – especially relating to access to restricted or classified documents – are drawn up as soon as possible after the adoption of the regulation.

Joint parliamentary scrutiny underlines the intrinsic link between Europol's work and national responsibilities for law enforcement.

Another aspect of controllability is the control suppliers of information to Europol have on the supplied data. The regulation introduces - similar as provided for in the Europol Council Decision - the possibility to place restrictions on handling or use: the handling codes. The possibility to impose such restrictions is an important instrument of trust enabling law enforcement authorities to supply Europol with data. Another instrument of trust in the Europol Council Decision is the provision of creating groups of Member States involved in a specific investigation: the analytical work file, focal point or target group. **The Europol Council Decision provides controllability for Member States participating in such projects¹⁹. The regulation does not have such provisions. Without controllability there is a clear risk that Member States will only contribute data with the highest restrictive handling codes making it impossible for Europol to fulfil its tasks.**

The JSB underlines that controllability is important from an operational and a data protection point of view: it defines who may participate and who may receive data from such investigations. **The JSB suggests that the regulation provides for clear provisions allowing controllability, especially in view of the new tasks for Europol.**

¹⁹ See e.g. Article 14(4 and 5) Europol Council Decision

7. Data Protection Supervision – controlling Europol’s data processing

The JSB stresses the need to maintain the strong involvement of the national DPAs in the supervision of Europol, while modernising the institutional arrangement. **The involvement of national DPAs is essential due to the fact that a very large majority of the data collected and processed by Europol originates from the Member States and will at a certain point also be sent back to the Member States**, albeit possibly in aggregated form or as part of an analysis report. The data streams between Europol and national law enforcement authorities are such that supervision simply cannot be strictly of a European nature. **The extensive national experience of how to deal with law enforcement information is required.** The limited role now foreseen for the national DPAs does not match their position vis-à-vis the law enforcement authorities. Also, no clear provisions have been created to stimulate joint enforcement actions, whereas that is one of the pillars of supervision in the data protection package. Furthermore, it is quite surprising that the Commission has decided not to include a role for the national DPAs, while at the same time roles are created or maintained for the national members of the Management Board, as well as for the national parliaments.

The specific role of Europol requires effective joint supervision including the national DPAs as well as the EDPS. The JSB therefore does not support the idea of the Commission to make the EDPS solely responsible for the supervision of Europol.

A coordinated supervision model is an option, but the model used for Eurodac, VIS and SIS II does not lead to the vigorous supervisor that is needed for Europol as it lacks the necessary requirements to truly enforce and ensure compliance with Europol's data protection legal framework.

It is the view of the JSB that the best way forward could be to create an independent and effective joint supervision structure with equal participation of each national DPA and the EDPS.

To ensure adequate supervision on a day-to-day basis, the JSB proposes that this joint supervision structure would be managed by a group of members (including the EDPS) who would meet frequently. This group - a standing committee - could also ensure regular contact with Europol and its Data Protection Officer, and act as appeals committee when the occasion arises.

8. Conclusion

The clearest conclusion that can be drawn is that the regulation, as it is currently formulated, would result in a weaker data protection regime at Europol. A downgrading of the regime would not only expose the organisation to risk; it would also endanger individuals' rights. There is much work to be done to improve the regulation and, in this first assessment, the JSB has highlighted the most urgent issues to be considered and has formulated some suggestions for change including a structure for effective data protection supervision. The JSB urges the European Parliament and the Council to ensure a legal framework containing a level of data protection appropriate for Europol and sufficient to protect individuals' rights

Done in Brussels, 10 June 2013

Natasa Pirc Musar

Chair