

Opinion of the Joint Supervisory Body of Europol

(Opinion 07/07)

**with respect to the proposal for a Council Decision establishing the
European Police Office (Europol).**

THE JOINT SUPERVISORY BODY OF EUROPOL,

A. Introductory remarks

On 20 December 2006 the Commission presented its proposal for a Council Decision establishing Europol.¹

Since this proposal has important implications for the processing of personal data by Europol, the Joint Supervisory Body of Europol (JSB) considers it as its task to present this opinion.

B. General remarks

The Justice and Home Affairs Council of 1-2 June 2006 concluded that competent Council bodies should commence work in order to consider whether and how the Europol Convention could be replaced by a Council Decision. In view of this, the Commission prepared a draft Council Decision establishing Europol.

In that Council meeting it was also concluded that in parallel with the debate on the new legal basis, the options for Europol's future as outlined in a Friends of the Presidency report² should be considered. As a result, the present proposal is not simply a copy of the Europol Convention including the three protocols amending that convention; it also contains some new elements relating to Europol's tasks and its information processing. In view of this, and taking into account the long

¹ COM (2006)817

² Council document 9184/1/06 of 19 May 2006

experience of the JSB with the functioning of Europol, this opinion shall cover all elements of the proposal: the already existing provisions, the amendments on existing provisions and those stemming from the Friends of the Presidency report.

In its assessment the JSB shall especially take into account the implications of the proposal for the information structure of Europol.

Data protection rules are imposed on Europol to protect the right of the individual whose data are processed by Europol. In its opinion on the third Protocol amending the Europol Convention³ the JSB emphasized that "*each organisation that processes personal data needs to invest and shall be hold responsible for decent processing of data, confidentiality, reliability and data quality In an area where Member States and Europol act in mutual cooperation and share information and intelligence, these obligations shall cover all the elements of cooperation and data-sharing*" The inspections of Europol which take place every year clearly demonstrate the importance of a well balanced system of data protection rules and clear responsibilities.

For this reason, the JSB shall also assess the effect of the proposal for the work of Europol and the shared responsibilities of the Member States and Europol in relation to the different aspects of processing personal data.

C. Specific Remarks

Relation with the Framework Decision on data protection

Article 26 of the proposal defining the standard of data protection refers to the principles of the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

The JSB together with all European data protection supervisors repeatedly stressed⁴ that there is a clear need for a harmonised and high standard of data protection in the Third Pillar. This high standard will function as a *lex generalis* and needs to be translated in specific data protection provisions (*lex specialis*) for Europol. The present proposal on condition that the suggestions made in this opinion are included may be seen as that *lex specialis* in which the specific position of Europol and the rights of the data subject are in balance.

At this moment it is however quite unsure whether the framework decision will be applicable to Europol and even what the content will be. In view of this situation and the need to have a high

³ JSB Europol opinion nr. 02-55, 3 October 2002

⁴ Krakow Declaration of 25-26 April 2005 and the opinion of the European Data Protection Supervisors on the proposal for a Council Framework Decision of 24 January 2006, London Declaration 2 November 2006.

level of data protection including the rights of individuals guaranteed in the draft Council Decision, the present proposal should include a comprehensive data protection regime.

Objective and competence of Europol

Articles 3 and 4 of the proposal introduce a distinction between the objective and the competence of Europol where the Europol Convention only refers to the objective of Europol. Although this may seem to be only a cosmetic change, its implications may be far reaching.

Europol's objective as defined in Article 2 of the Europol Convention limits Europol's activities to certain well described types of crime with an international character and when a criminal organisation is involved, thus limiting Europol's competence and activities to these crimes.

The proposal introduces a general description of the types of crime falling within Europol's objective followed by adding certain conditions to these crimes (affecting two or more Member States, in particular organised crime and terrorism) when describing Europol's competence.

Europol's objective thus covers more criminal activities than those for which Europol is competent according to Article 4 of the proposal. This obviously creates a discrepancy between the objective and the competence of Europol.

The explanatory memorandum to the proposal as well as the Friends of the Presidency report does not clarify the reason for this distinction. The report only mentions that the area of competence and specific tasks of Europol are not clearly defined in the Europol Convention.

The JSB stresses that such a distinction may have its consequences for Europol and the Member States. For example, this distinction may be interpreted as if Europol is an organisation in which Member States operate to fight serious crime (the objective) and in which Europol has its own role and competence when these crimes have an international character (the competence). It thus describes a platform for Member States to cooperate with each other and with Europol when it concerns crimes falling within Europol's competence. Article 9(2) of the proposal describing the possibility for liaison officers to exchange data on a bilateral level using Europol's technical infrastructure on crimes outside the competence of Europol apparently supports this. This may however have far reaching consequences for the future work of Europol as an organisation (also facilitating Member States cooperation outside Europol's competence. This may have serious implications for the data protection responsibilities of Europol. For example, may Member States use Europol's analysis tools and systems and even officials when cooperating on a bilateral level? And if so, who will be then responsible for data protection issues as the quality of data, retention periods, access to these data and the rights of the individual? Moreover, will Europol also be

responsible for making available secure information structures for exchanging data between Member States and even with third parties and as such operating as intermediary?

Conclusion: the JSB stresses that it should be clarified why the distinction is made between the objective and competence of Europol and which consequences this might have for the information structures within Europol, with Member States and third parties.

Furthermore, the proposal may create difficulties when interpreting Europol's competence. The Europol Convention stipulates that two or more Member States must be affected by the crime in such a way as to require a common approach by the Member States owing to the scale, significance and consequences of the offences concerned (Article 2(1) Europol Convention). Using the condition that "a common approach" is required is necessary to clearly determine when Europol will be competent.

Article 4(1) of the proposal only refers to serious crime affecting two or more Member States. This is clearly a less distinctive condition. Serious crime may occur in one Member State and even affect another Member State but that does not always require a common approach. The present text will no doubt create uncertain situations when Europol will be competent to act and even when assessing which data may be entered in the Europol Information System. The JSB furthermore notes that the proposal does not repeat the condition in the Europol Convention that there should be factual indications or reasonable grounds for believing that an organised criminal structure is involved. In its opinion on the third Protocol amending the Europol Convention, the JSB already noted that this deletion may be motivated by experience in dealing with serious crimes involving more than one Member State.

Conclusion: the JSB suggests bringing Article 4(1) more in line with the present text of the Europol Convention, taking into account that the JSB already accepted that the existence of a criminal organised structure is not a limiting element anymore.

Article 4(3) of the proposal describes offences which shall be regarded as related criminal offences falling within Europol's competence. It copies the description as used in the Europol Convention with one exception: the exclusion of offences predicate to money laundering activities with regards to which forms of crime Europol has no competence⁵. The explanatory memorandum does not

⁵ Money laundering in general is defined as serious crime in Annex I of the draft Council Decision

provide for an explanation for this and it is also not a suggestion made in the Friends of the Presidency report.

Since no clear motivation is presented why Europol's competence with money laundering should also imply enlarging its competence to predicate activities which in itself do not fall within Europol's competence and even not necessarily within the objective, expanding Europol's competence is not based on a clear and transparent assessment.

Conclusion: the JSB strongly suggests including the exception for offences predicate to money laundering activities in the description of related offences.

Tasks

Article 5 describes Europol's tasks. The tasks as defined in Article 3 of the Europol Convention are copied in the proposal but some new tasks are added.

The JSB shall only comment on the new tasks.

Article 5 (1)(a)

Europol receives information it needs from the national units or from designated competent authorities (Article 4(2) Europol Convention)⁶.

Responsibility for the legality of the collection, transmission to Europol and input of data, their accuracy, their up-to-date nature and verification of storage limits shall lie with the Member State that communicated these data (Article 15(1) Europol Convention). The combination of the central role of the national units or designated competent authorities with the responsibilities of Member States provides for a clear and transparent system of controlling the exchange of personal data with Europol.

This concept is also used in Article 5 and 28 of the proposal. However, Article 5(1)(a) opens the possibility for Europol to receive information from third countries or public or private entities.

Receiving data from public or private entities is an existing wish and it is one of the suggestions in the Friends of the Presidency report (point 22 in the matrix). The JSB recognises the need for Europol to receive and use these data in specific cases and analysis projects.

However, the opportunity for Europol to receive data from these sources raises the following questions: i) is Europol entitled to approach those public and private entities directly? ii) what will

⁶ Protocol amending the Europol Convention, OJ C 2, 6.1.2004, entering into force 18 April 2007

be the legal basis for providing the information? and iii) who will be responsible for the lawfulness of the communication?

i) The proposal apparently intends to allow Europol to approach public and private entities directly. There is no specific obligation to direct such requests to national units or to have specific arrangements in place as referred to in Article 22 of the proposal dealing with Community or Union related bodies and agencies. Although the JSB does not dispute the necessity to involve data from these entities in specific investigations in which Europol is involved, it seems that this proposal introduces a concept of availability of data processed by public and private entities as basis for allowing Europol to directly approach these entities⁷. It is furthermore not logical that Europol is obliged to contact national units or designated authorities when collecting law-enforcement information but it is free to directly contact other parties. In this respect it should be noted that data from public and private parties may have the same degree of sensitivity as law enforcement data (e.g. DNA data, data about asylum seekers). From a control point of view such diverse contacts in collecting information are not advisable.

ii) An aspect closely related to point i) is the legal basis for providing the information. When it concerns personal data, the requested party shall be bound to the obligations of Directive 95/46 EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁸ and its implementation in national law.

This directive contains a fundamental principle on the lawfulness of the processing of personal data: data should be collected for explicit and legitimate purposes and not further processed in a way incompatible with those purposes. An exemption or restriction is only allowed when provided for by law and when this constitutes a necessary measure to safeguard national and public security or the prevention, investigation, detection and prosecution of criminal offences. This exemption should thus be provided for by national law. The JSB has no overview on how this exemption is implemented in the national laws of all Member States and also no information whether the existence of such exemptions also includes the transmission of personal data to an international organization as Europol. It should also be stressed that the mere fact that the proposed Council Decision allows Europol to collect and process such data is in itself not a sufficient legal basis for public and private entities to transmit data to Europol. It shall thus be difficult for Europol and the requested parties to assess whether they will be allowed to collect or communicate these data.

⁷ See explanatory memorandum, page 5, last paragraph

⁸ OJ L 281, 23.11.1995, p.31

iii) Further to the observations under i) and ii) it seems logical to maintain the system as defined in Article 28 of the proposal concerning the responsibility in data protection matters of Member States which communicated the information (including information from public and private parties since Article 28 makes no distinction between the sources of data). Member States can only take up this responsibility when they are involved in the collection of the information by Europol.

When it concerns data-collection from open sources, the JSB considers it to be logical that Europol is in the same position as other law-enforcement authorities and could retrieve data from these sources directly.

Conclusion: the JSB supports the possibility for Europol to also process personal data made available by public and private entities under the condition that the requests for such information is directed to the national units (with the exception of data from open sources). It will be the task of these units to assess together with the requested party whether, based on national law, such a request could lead to the transmission of personal data. Article 8(2) of the proposal dealing with the national units should provide for this specific task.

Article 5 (1) (b) and (f)

These two subparagraphs introduce new tasks for Europol. The JSB stresses that any task of Europol involving the processing of personal data should comply with the data protection provisions applying to Europol. These provisions include a clear definition of the responsibilities of Europol and Member States for data processing. Both new tasks seem to implicate that Europol's activities may also take place in the Member States. Article 28 dealing with the responsibilities in data protection matters, now only distinguishes the responsibilities of Member States and Europol when processing data at Europol.

It will be important to guarantee that Europol's activities as referred to in these two subparagraphs may only take place within the sphere of Europol's competence and within the framework of Europol's data protection framework. These activities must be covered by the rules applying to Europol in a similar way as for Europol's participation in joint investigation teams.

Conclusion: Article 5 and Article 28 should be brought in line with each other, specifying the different data protection responsibilities when Europol's data processing activities take place outside the Europol premises. Europol's activities must be covered by specific provisions similar as for Europol's participation in joint investigation teams.

Article 5 (2)

Another new task is monitoring the internet to assist in the identification of certain criminal activities. This kind of activity will no doubt lead to the processing of personal data. It is not sure whether such processing will take place in the framework of the analysis files as referred to in Article 14 of the proposal or that another form of processing is foreseen. It is also not clear whether the present proposal of Germany for a "Check the Web" project⁹ is an example of this new task of Europol. In case the legal framework of analysis files is not used for this task, the proposal should either contain the necessary description of the information structure to be used for this task including the necessary data protection provisions, or it should include a clear reference to the procedure as referred to in Article 10(3) of the proposal.

Conclusion: the proposal should contain a clear description of the information structure for monitoring the internet or a reference should be made to Article 10(3).

Participation in joint investigation teams

Article 6 describes Europol's possible role in joint investigation teams. Since the protocol amending the Europol Convention introducing this participation is not yet in force (it will enter into force on 29 March 2007) there is no experience yet with the new Article 3A of the Europol Convention.

In view of this, the JSB does not understand why the proposal does not maintain in general the specific limitation of Europol's role in joint investigation teams to the investigation of criminal offences for which Europol is competent (Article 3A of the Europol Convention).

Conclusion: the JSB emphasizes the need to maintain that limitation in Article 6 of the proposal.

National units

Article 8 of the proposal describes the tasks of the national unit. These tasks are no different than in the Europol Convention. However, Article 8 (2) is not similar to Article 4 (2) of the Europol Convention describing the liaison function of the national unit. Article 4(2) of the Europol Convention will enter into force on 18 April 2007. The JSB wonders why the obligation to inform the national units in case information is exchanged between designated authorities and Europol is not maintained. Since there is no experience yet with these direct contacts it seems strange to

⁹ JHA Council 4-5 December 2006

already delete this obligation. It should also be stressed that Member States benefit when their national units are informed thus allowing them to better control data transmission that falls under their responsibility. At the same time, the national data protection supervisors have one point of control when supervising the data transmission to Europol.

Conclusion: the JSB urges to maintain the provision of informing the national units as provided for in the new Article 4(2) of the Europol Convention.

Liaison officers

Article 9 of the proposal describing the position and tasks of liaison officers has great similarities with Article 5 of the Europol Convention. There is however an important difference: Article 9(2)(d), second sentence, also allows exchanging information with liaison officers of other Member States about crimes falling outside the competence of Europol (see also JSB's comments on the objective of Europol). This may perhaps be legalising a practice that probably already exists. The JSB understands that the presence of so many liaison officers of all Member States within Europol will automatically create a platform for cooperation including the sharing of information on a bilateral level. It should however be noted that for the exchange of information between national units and liaison officers, technical facilities of Europol are used and may be even involving Europol's officials. Although the situation as described may seem logical from a general law-enforcement perspective, the question remains whether facilitating such exchange is to be regarded as a task for Europol and if so whether Article 5 of the proposal should not explicitly include this task. It should furthermore be made clear that although Europol may have the task of facilitating bilateral information exchange, Europol has no responsibility for the content of the exchanged information.

Conclusion: Article 5 of the proposal should specifically mention this task. Article 28 should contain a specific provision on the responsibility for the exchange between liaison officers.

Information processing

Article 10 of the proposal introduces a general provision on information processing at Europol. It mixes the present Article 6 of the Europol Convention and the new Article 6A of that convention with some new provisions. These new provisions create the possibility to define other systems of data processing.

Article 10(1) obliges Europol to establish and maintain the Europol Information System and analysis work files. The index system as referred to in Article 6 of the Europol Convention apparently does not exist anymore as a separate defined system and is further referred to as the index function in Article 15 of the proposal.

Article 10 (2) of the proposal allows Europol to process data to determine whether they are relevant for its task and can be included in one of its information systems. The JSB wonders why the text of the proposed Article 10(2) does not follow the same structure as in Article 6A including all the necessary safeguards. The present proposal as such is not specific enough and may lead to uncontrolled and undefined data processing and will for this reason be unacceptable. An alternative solution might be to regulate all handling of personal data by Europol in specific provisions providing new additional safeguards for personal data (e.g. use of specific codes for accepted data revealing the scope and/or purpose of communication).

Conclusion: the JSB strongly suggests bringing Article 10(2) in line with the new Article 6A of the Europol Convention, or to regulate all handling of personal data in specific provisions.

Article 10(3) opens the possibility for Europol to establish other information systems than referred to in Article 10(1) of the proposal. This provision intends to create more flexibility for Europol to react effectively to new developments and law-enforcement demands. The JSB understands that there might be a need for flexibility, but such flexibility should comply with the necessary high data protection standards and the principle of proportionality. The procedure for determining the conditions under which Europol may establish new information systems provides for sufficient guarantees to protect the interests of data subjects.

However, the JSB notes that one of the most fundamental data protection principles: the definition of the purpose of the data processing is not included in the list of these conditions. The JSB urges to include the purpose definition in Article 10(3).

In view of its specific expertise the JSB should be consulted on the initiatives to establish new information systems at Europol.

Conclusion: Article 10(3) should also mention the purpose of the information system; an obligation to consult the JSB should be introduced either in Article 10 (3) or in Article 36(12).

Article 10 (5) introduces an obligation for Europol to make every effort to ensure that its data processing systems are interoperable with data processing systems in the Member States and those

in use by Community and Union related bodies especially by following best practice and using open standards.

Although it seems logical to improve an efficient exchange of information by introducing interoperability of systems, the JSB stresses that this technical interoperability does not automatically mean that data may actually be exchanged. Exchange should only take place in the framework of the proposed Europol Decision and the legal provisions of the system with which a link will be proposed. Any new proposal for exchange of data using interoperability should be assessed on its own merits.

In order to ensure that decisions to technically link Europol systems with either national systems or from other institutions are based on an assessment whether the exchange following the connection between systems is legally possible, a decision to create such a link may only be adopted after consultation of the JSB and the data protection supervisor of the Member State or Community or Union body involved.

Conclusion: Article 10(5) should include the obligation to consult the JSB and other involved data protection supervisor(s) before a decision is made to interlink Europol's information systems with other systems.

Europol information system

Article 11 describes the existence of the Europol Information System, the different responsibilities of Europol and the Member States and the access to this system. The proposal follows in general Article 7 of the Europol Convention. A significant change however is introduced by deleting the restriction of the direct access for national units to data relating to persons of whom it is believed that they will commit crimes in the future. The data to which access is now allowed according to the Europol Convention concern the details of the identity of a person. Other data will only be made available for a specific enquiry.

The deletion of this limitation is one of the subjects mentioned in the Friends of the Presidency report. According to that report it is considered a problem that national units do not have the same access privileges to all information in the Europol information system as Europol officials.

The JSB stresses that a wish for having equal access privileges is not a crucial element to be taken into account when deciding on access to the Europol information system. Although Member States are cooperating within Europol this does not implicate an unconditional access to all data processed by Europol. Law-enforcement officials should only have access to data when necessary for their task in a specific case. Furthermore, the categories of data should also be taken into account. Access

to and use of certain categories of data should be limited when the nature of these data so require. This is especially the case when it concerns suspicions about possible future behaviour of individuals. Access to this specific category of data should always be limited to a need for a specific enquiry with specific control mechanisms to ensure this limitation.

It should also be stressed that this limitation does in principal not only regard the national units but all officials including those from Europol. However, in view of Europol's responsibility for the Europol Information System and the execution of Europol's tasks as referred to in Article 5(1) it seems logical that some Europol officials have access rights to all information processed at Europol. The reference in Article 7(1) of the Europol Convention to duly empowered officials already indicates that not all Europol officials will have access.

Conclusion: the JSB strongly suggests maintaining the limitation of the access as referred to in Article 7(1) of the Europol Convention in Article 11 (1) of the proposal.

Content of the Europol Information System

Article 12 of the proposal describes the content of the Europol Information System and follows in general Article 8 of the Europol Convention. The content of the system is related to criminal offences for which Europol is competent. However, the proposal does not exclude anymore the processing of data concerning related offences as is the case in Article 8(1) of the Europol Convention. This is a new element in the proposal and it is not motivated either in the explanatory memorandum or in the Friends of the Presidency report.

In view of the definition of related offences in Article 4(3) of the proposal and taking into account that the related offences also include all offences predicating to money-laundering activities (see comment JSB on Article 4(3) of the proposal) the question arises on which moment a conclusion can be made that a criminal offence may be regarded as a related criminal offence. Is this only after assessing that a certain crime falls within the scope of Article 4(1) and (2) and that there are related offences or is the mere change that a criminal offence may be a related offence provides for legitimating processing in the Europol Information System. This creates a clear risk that data will be processed on subjects and offences of which there is no certainty that it concerns related offences as referred to in Article 4(3) of the proposal. The JSB also refers to its comments on Article 4(1).

The JSB stresses that the processing of data concerning related offences may only be justified when it is assured that they are related to offences for which Europol is competent. The present system of Article 8(1) and (4) should thus be maintained and the processing of related offences should be excluded.

Conclusion: in Article 12 of the proposal the exception for processing data on related offences and a provision for marking additional information on related offences as foreseen in Article 8 of the Europol Convention should be included.

Analysis Work Files

Article 14 of the proposal is almost identical to the provision on analysis work files in the Europol Convention. The JSB has no specific comments on this article.

The JSB further refers to the letter sent to the Chairman of the Europol Working Party¹⁰ in which it raised the question whether maintaining the same legal provisions as those in the Europol Convention for Analysis Work Files will continue to reflect the necessary balance between the different needs of crime analysis and of data protection. The present rules were developed in the period 1993-1995 and were partly changed by the third protocol of 2004. It subsequently suggested to evaluate the present framework for analysis files and to develop a vision for the future tasks of Europol involving various products of crime analysis.

Index function

The index function for data stored in the analysis files is described in Article 15 of the proposal. It follows with some exceptions the structure of the provisions on the index system as described in Article 11 of the Europol Convention. The JSB welcomes the formalisation of the practice that the Management Board seeks the advice of the JSB when defining the design of the index function.

A first observation relates to the name "index function". The JSB understands that the proposal intends to highlight more the functionality of an index on the content of the analysis files. This change should however also be assessed in relation to Europol's obligations concerning its automated data files. By introducing an index function in place of the index system there might be a discussion whether the index function should be considered as an automated data file as referred to in Article 18 dealing with the controls on retrievals. The Europol Convention foresees in Article 6 and Article 16 that retrievals from the index system are subject of appropriate control mechanisms. Since the index function is not defined anymore in Article 10 of the proposal and the reference in Article 18 of the proposal to automated data files may lead to discussions whether it also applies to index functions, it should be ensured that Europol should also establish control mechanisms of retrievals using the index function.

¹⁰ Letter 07-04 of 26 January 2007

Conclusion: Article 18 should explicitly mention the index function.

Another aspect of the proposal in which it differs from the Europol Convention is the use of the word "access" instead of consultation. Access implies direct access where the right to consult more qualifies what may be consulted without combining that with having direct access. The JSB wonders why in the proposal the consultation has been replaced by "access".

The JSB furthermore notes that the group of officials having access privileges to the index function is extended with duly empowered officials of the national units. The JSB assumes that it will be the national units to decide who will be empowered. Since introducing these access rights for the national units is not explained in the explanatory memorandum or mentioned in the Friends of the Presidency report, the JSB wonders about the motivation to provide those units with access to the index function. In principle an assessment whether national units should have access must take into account the concept of analysis files, their content, the need for national units to be informed whether data on an individual is processed in the analysis files and the already existing possibility for Member States' liaison officers to be informed by using the index function (Article 15 (2) in relation with Article 14(5) of the proposal).

This assessment should also take into account that a query in the index function only reveals whether data on an individual are processed in an analysis work file. It however does not reveal in which category of persons (suspect, witness, victims) these data are processed (see also Article 15(3)).

The JSB furthermore understands that there is no clear and uniform structure for national units. It may range from having a single central unit in a Member State to a very large group of officials working in various law-enforcement organisations of a Member State. Providing the privilege of access to national units may thus lead to claims for creating such access in numerous places for a perhaps unlimited amount of officials in Member States.

In view of the content of analysis work files, the necessary control on retrievals (Article 18), the possibility for liaison officers to consult the index function and the undefined structure of national units, the JSB cannot find a justification for granting access privileges to national units.

Conclusion: the JSB stresses that retrieving information from the index function should be limited to those officials as referred to in Article 11 of the Europol Convention.

The JSB also draws the attention to the following. Data processed at Europol may be accompanied by so called handling codes. Although these codes are in principle serving an operational interest, they may coincide with a data protection interest. When such codes intend to limit the transmission of these data subject to prior approval of the Member State responsible for the input of these data, the dissemination of that information through the index function may appear to be counter productive. The JSB refers to its observations about equal access rights and the access to the Europol Information System.

Conclusion: the JSB suggests to explore whether Article 15(2)(3) should distinguish between data to which access is not limited and data which have a specific handling code aimed to prevent access without prior approval.

Order opening an Analysis Work File

Article 16 describing the order opening an analysis work file follows with some exceptions the same provisions of Article 12 of the Europol Convention. The JSB has no comment on the changes.

Experience with analysis work files demonstrates that such files are not static files. Participants may change and even the categories of data to be processed may be subject of change. However, the present provisions of the opening order only refer to the situation at the beginning of the work file. Since the opening order is an important instrument for creating transparency about the specifics of that file for all involved, this instrument must always be updated when changes are introduced. The JSB therefore suggests introducing an obligation to amend the opening order whenever changes take place on the subjects as referred to in Article 16(1) of the proposal. The Management Board and the JSB should always be directly informed about such changes.

Conclusion: Article 16 should include an obligation to amend the opening order when a change takes place concerning the subjects referred to in Article 16(1) including an obligation to directly inform the Management Board and the JSB.

Provisions on control of retrievals

The JSB refers to its comments on the index function.

Time limits for the storage and deletion of data files

Article 20 describing the time limits for the storage and deletion of data files follows with some exceptions the same provisions of Article 21 of the Europol Convention.

Article 20(1) provides for the general rule for reviewing the continued storage of data in all Europol's data files. Since the proposal introduces the possibility for the Council to determine the conditions under which Europol may establish other systems than defined in the present proposal and since those conditions may include shorter periods for reviewing, Article 20(1) should include a linking clause with Article 10(3) of the proposal.

The JSB is concerned about the deletion of the specific provision for reviewing data in the analysis work files. This specific provision is introduced by the third protocol amending the Europol Convention¹¹ and is a crucial part of the restructuring of the provisions concerning the period of storage of data in analysis work files (now Article 16(4) of the proposal). Analysis work files may now exist as long as the need for continuation of the file is justified. In view of this, the risk of maintaining data no longer needed for the analysis process and the possible impact crime analysis may have for an individual present a clear need for an annual review. Deletion of this provision is therefore unacceptable. The JSB emphasises the need to have an adequate system of reviewing in place. Such a review could perhaps take place on the moment of using information or adding new information instead of only on a fixed moment.

Conclusion: Article 20(1) should include a linking clause with Article 10(3) of the proposal. The obligation for an annual review of data in analysis work files or another adequate system of reviewing should be introduced.

Correction and storage of data in paper files

Article 22 of the Europol Convention contains specific rules for the correction and storage of data in paper files. It also defines specific rights for persons covered by those files. The present proposal does not include such a specific regime. The JSB repeats its observation concerning the relation between the Framework Decision on data protection and the Europol Decision and its conclusion that the draft Council Decision should provide for a comprehensive data protection regime.

¹¹ OJ C 2, 6.1.2004, entering into force 18 April 2007

Conclusion: the specific rules of Article 22 of the Europol Convention concerning the correction and storage of data in paper files should be included in the draft Council Decision.

Access to national and international databases

Article 21 is a general provision allowing Europol to gain computerised access and retrieve data from international and national information systems. Article 10(5) of the Europol Convention contains the same provision but limited to the processing of data in analysis files. The proposal thus has a wider impact for data processing at Europol relating to all tasks referred to in Article 5 of the proposal and all information systems referred to in Article 10(1)(2) and (3). Although Union, international or national legal instruments will apply to the computerised access, the proposed Europol Decision also needs to provide for clear rules on the use of such computerised access. A provision that access will only be possible on a case-by-case basis and for crimes falling within Europol's competence is essential for a controllable use of the computerised access.

Furthermore, it should be made transparent when access to national and/or international data bases is provided for and used. Both on a national level as well as for those authorities supervising the international data bases information on this access should be made available. The actual use of this access should be sufficiently logged and audited.

Conclusion: Article 21 should stipulate that computerised access is only allowed for the execution of Europol's tasks and within Europol's competence on a case-by-case basis.

Communication of personal data to third bodies

Article 24 (1) (b) allows the Union to conclude international agreements with third bodies in which the assessment of the existence of an adequate level of data protection is ensured. Similar as in the present situation in which the opinion of the JSB on the adequacy level is needed before the Council may allow the Director of Europol to conclude such an agreement, a consultation of the JSB should be included in Article 24(1) (b).

The JSB furthermore notes that paragraph 2 gives the Director of Europol the possibility to derogate in specific cases from the principles of Article 24. However, both Article 24 (2) and (3) do not contain an obligation to inform or consult the Data Protection Officer and/or the JSB of the use of this derogation. In view of the importance of a proper assessment of the adequacy level, it is important that the JSB or at the very least the Data Protection Officer is consulted when the Director is assessing the adequacy of data protection afforded by third bodies. In case the urgency of the matter does not allow prior consultation, the JSB should be informed after the event.

Conclusion: Article 24 should provide for a consultation procedure with the JSB.

Data Protection Officer

The JSB welcomes the formalisation of the function of a Data Protection Officer. It emphasises the need for an organisation as Europol to institutionalise such a function and the need for such an officer to act in a completely independent way.

Responsibility in data protection matters

Article 28 of the proposal defining the data protection responsibilities for data processing at Europol has caused some concerns in the recent past. Furthermore, some of the new provisions in the proposal also need specific regulation of this responsibility.

Based on its experiences with data processing at Europol, it has become clear that even when Member States have a responsibility as defined in Article 28 (1), this does not exclude Europol's own responsibility for data processing. Especially in situations where Member States input data in one of Europol systems, Europol should also have the responsibility to act when it establishes that the data processing is not in compliance with the proposed Europol Decision. Europol should at least warn the inputting Member State about its doubts. This is clearly the case with the Europol Information System but it may also apply to any new form of data processing as referred to in Article 10(3) of the proposal.

Furthermore, the provisions for Europol to have computerised access to other systems, and the possibility to receive information from European Institutions need to be accompanied with specific provisions on the responsibility for these data.

Conclusion: Article 28(1) should further define Europol's responsibilities in combination with those of the Member States, in those situations where Europol has computerised access and when receiving information from European institutions.

Rights of the data subject

The right of access to personal data and the right to have these checked are foreseen in Article 29 of the proposal. Experiences with the present provisions, which for an important part are also included in the present proposal, are not that positive. This is in particular the case where both the national law of the Member State in which the right is invoked and the provisions of the Convention (and now the proposed Council Decision) apply. Apart from the practical problems for Europol to also

deal with a request in accordance with one of the twenty five (and soon 27) national laws of the Member States, an evaluation of the decisions of the Appeals Committee (Article 24(7) Europol Convention) demonstrates that in some cases Europol's decision on a request for access was considered being in compliance with the Europol Convention where in other identical cases Europol's decision was assessed as being non-compliant. The difference was caused by the application of the different national laws. This is a clear indication that a more harmonised European approach on the right of access and certainly concerning data processing by the European Police Office is really needed. However, such a harmonised approach should not be at the expense of guaranteeing a high level of data protection.

The JSB stresses that in the execution of its tasks, Europol is only bound by the provisions of the Europol Convention and not also to national laws. This clear demonstration of mutual trust between Member States and Europol in proper processing of personal by Europol should also exist when dealing with fundamental data protection rights.

The present proposal is certainly not in line with such an approach. It not only maintains the system that national law should be applied; it also introduces the possibility for Member States to object to giving access in analysis work files not only when they are participating in such a file but also when they are directly concerned by the communication of the data. Especially this right to object for such a wide group of "concerned parties" would in practice mean that it is unlikely that access will ever be allowed. The JSB understands that a right of access and the interests of law-enforcement should be balanced in a careful way. However, the fact that Europol processes data transmitted to it by Member States does not lead to the only conclusion that Europol should also apply Member States national law when dealing with data subjects rights.

The proposed Council Decision should thus provide for the necessary provisions guaranteeing the fundamental data subjects rights of access and to have data checked. Whilst the JSB understands the need for exceptions, the use of these exceptions should only be used when proven to be necessary in a specific case. The reasons for refusal as referred to in Article 19(3) of the Europol Convention in combination with the condition that refusal must be necessary for these reasons are generally accepted in international data protection and law-enforcement legal instruments. In view of this, the JSB proposes to replace the present provision of Article 29 of the proposal with a uniform legal provision dealing with the rights of the data subject in which Europol only applies that provision and not in combination with national laws.

Since Europol is expected to decide on every request on a case-by-case basis, such a provision may also include an obligation to consult Member States directly involved. In case a Community or Union related body or agency is involved, this consultation should also apply that body or agency.

The JSB is furthermore concerned that a three months period as referred to in Article 29(3) is an unreasonably long time for Europol to deal with a request for access. The request should be dealt without undue delay (e.g. within one month).

Conclusion: the Council Decision should provide for a comprehensive harmonized provision guaranteeing data subjects a high level of rights of access and to have data checked without the applicability of national laws. Such a provision can also include a provision for Member States or Community institutions directly involved to state their opinions but these should not necessarily be overriding. The time limit for Europol to respond to a request for access should be very much less than three months.

Correction and deletion of data

Article 30 provides a data subject the right to have his data corrected and deleted. This provision is similar as the provision of Article 20 of the Europol Convention. The JSB suggest including in paragraph 2 an obligation for Community or Union related body or agency to correct or delete data.

Conclusion: The JSB suggest including in paragraph 2 an obligation for Community or Union related body or agency to correct or delete data.

Appeals

The provision giving a data subject the right to lodge an appeal against Europol's decision on a request for access or for a check forms an important guarantee for independent ruling on Europol's decisions. Article 31 of the proposal follows Article 19 (7) and (8) of the Europol Convention. In view of the remarks made about the rights of the data subject, the present proposal should be amended. A decision in appeal should be a decision whether Article 29 and 30 of the proposal are applied correctly. Since it is suggested by the JSB not to also include an assessment by Europol of national laws of the Member States this should also be excluded in the appeals procedure.

Conclusion: the provision dealing with the appeals should be brought in line with the JSB suggestion on the rights of the data subject.

General conclusions

The proposed Council Decision establishing Europol contains some fundamental changes in comparison with the Europol Convention.

The JSB understands that there might be a need for flexibility, but such flexibility should comply with the necessary high data protection standards and the principle of proportionality. Some of the suggestions in the Friends of the Presidency report are introduced in the proposal, and some changes are introduced without any specific motivation.

The JSB has presented its observations and is convinced that the present proposal on condition that the suggestions made in this opinion are included may contribute to a more effective cooperation between Member States and Europol in which the protection of personal data is sufficiently guaranteed.

The JSB is aware of the fact that further discussion concerning the functioning of Europol and the cooperation between Member States may lead to new amendments of the present proposal. The JSB stresses that it should be informed of any amendments to these proposals and be given the opportunity to state its opinion. The JSB would like to emphasise its readiness to cooperate as appropriate.

Done at Brussels

5 March 2007

David Smith

Chairman