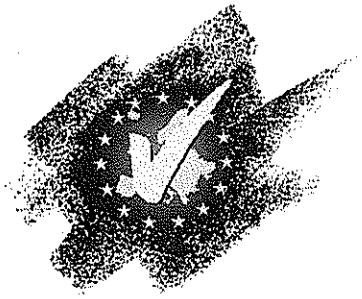

EUROPOL JOINT SUPERVISORY BODY

Second Opinion of the Joint Supervisory Body of Europol (JSB)

(Opinion 13/56)

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)

Rue de la Loi 175 - Bureau 0070FL59 - B-1048 Brussels
Phone: +32(0)22815026 - Fax: +32(0)22815126

MANAGEMENT SUMMARY

In this second opinion on 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) (hereinafter: the regulation), the JSB focuses on the consequences of the various provisions in this proposal on Europol's operational activities and on data protection. Linking these two areas is essential for a better understanding of the impact of these provisions. Europol's robust data protection system under the Council Decision of 6 April 2009 establishing Europol (hereinafter: Europol Council Decision) was based on specific data protection provisions relating to its various data processing activities. The proposal changes this.
This second assessment confirms in detail the conclusion of the first JSB opinion that the data protection level presented in the regulation is much weaker than the one provided for by the Europol Council Decision. This assessment also confirms that the regulation will not achieve the intended flexibility for Europol to achieve its tasks. The flexibility instrument combined with effective data protection measures offered by the Europol Council Decision already allow Europol to be more flexible.

Many comments are based on the tasks Europol is now performing or needs to perform in the near future. The evolving nature of Europol's work requires its objectives and tasks to be reassessed. The JSB suggests several changes to allow Europol to perform current (and future) tasks under tailor-made data protection provisions.

The main issues further discussed in this opinion include:

The present text of **Article 3** describing the objectives is not sufficient to encompass all Europol's present and future activities. There is a clear need to introduce specific rules and effective guarantees for an accountable organisation for such activities as well. The JSB suggests re-assessing and amending Article 3 in such a way that Europol's objectives better fit its present and expected future role.

In its assessment of **Articles 24-25**, the JSB warns that there is a clear risk that the proposed regulation will not enable Europol to fulfil its main task of strengthening mutual cooperation between Member States and other parties in the best possible way where operational interest and data protection are in balance. The JSB suggests assessing whether the present structure could be improved and where necessary made even more flexible.

Another aspect that is highlighted in this opinion is **Member States' lack of influence** over what will be done with the information sent to Europol. This is especially the case with direct contacts between Europol and law enforcement authorities and the exchange of information with Europol's partners. **The JSB considers it not a balanced approach when the approval of Member States is assumed when a Member State did not explicitly objects against a further transmission.** In view of the data protection implications involved, the JSB advises that this approach be reconsidered.

Concerning the long-awaited solution for exchanging information between **Europol and European Union police missions**, the JSB concludes that the provision introduced for making such exchange possible lacks sufficient safeguards.

The JSB repeats that it does not support the Commission's idea of making the EDPS solely responsible for the **supervision of Europol**. As also stated by the conference of European Data Protection Authorities, effective data protection supervision of Europol cannot be done without the strong involvement of the national DPAs. The JSB highlights the importance of establishing an independent and effective joint supervision structure with the equal participation of each national DPA and the EDPS. This joint supervision structure must be independent and have the necessary powers to fulfil its tasks.

The JSB comments on most articles dealing with the processing of data. These comments are based on long years of experience with Europol's work and data protection. Where possible the JSB gives suggestions for an amendment; other suggestions are directed more towards reconsideration.

The JSB is of course always prepared to give further advice and assistance.

1. Introduction

On 10 June 2013, the Joint Supervisory Body of Europol (JSB) presented a first opinion (hereinafter: Opinion 13/31) on the draft 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).

In that opinion the JSB concluded that the regulation would result in a weaker data protection regime at Europol, not only exposing Europol to risks but also endangering individuals' rights. The various comments made by the JSB concerning data protection, Europol's role and responsibilities, its tasks, the choice of processing environment, controllability and data protection supervision form the basis for this second opinion, in which specific comments will be made in relation to particular articles of the regulation.

These comments should thus be read in the context of the general remarks made in the first opinion.

2. Comments on specific articles

Article 2, definitions

(a) The regulation introduces a new definition of "competent authorities". The JSB notes that this definition differs from that used in Council Framework Decision 2008/977/JHA and that proposed in the draft Directive 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. Also, it apparently allows an authority that is not a public authority to be considered a competent authority.

Since the definition of competent authorities in Article 3 of the Europol Council Decision has not led to any problems, the JSB suggests maintaining that definition.

---

[1] COM(2013) 173 final

(b) The definition of data "analysis" is too broad and is not distinguished sufficiently from the general concept of data processing as used in the existing data protection legislation. Since analysing data is an important aspect of Europol's work and is the purpose of information processing activities, a precise definition is needed. A definition used by Europol to define analysis is: the careful examination of information to discover its meaning and essential features. The JSB suggests aligning the definition used in Article 2 with what is generally accepted as crime analysis in the area of law enforcement. This is also important in relation to Article 24 of the regulation describing the purposes of information processing activities.

(c) The definition of "Union bodies" mentions institutions, entities, missions, offices and agencies set up by or on the basis of the Treaty on European Union and the Treaty on the Functioning of the European Union. The JSB notes that this definition widens the scope of what is generally considered as a Union body, to include entities and missions. The Europol Council Decision, for example, only refers to "institutions, bodies, offices and agencies"[1]. In a recent legislative proposal for the Eurojust Regulation[2], only Union bodies and agencies are mentioned in the chapter dealing with relations with partners. These differences are not without importance, since the definition is apparently intended to enlarge the group of recipients of Europol data. The JSB refers further to its comments on Articles 4 and 29.

(f) The definition of "international organisations" in the Europol Council Decision refers to "other bodies governed by public law which are set up by or on the basis of an agreement between two or more States". The definition in the regulation does not link these other bodies to public law anymore. Since there appears to be no reason for this change, the JSB suggests maintaining the definition provided in the Europol Council Decision.

(k) The regulation defines who should be regarded as a "recipient" following the definition used in the present proposals for a data protection package[3]. However, it adds that "authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients". Such an exemption is not justified and also not logical in view of the rights and obligations incumbent on recipients as defined in the regulation in Articles 30, 39 and 41. The JSB strongly suggests deleting this exemption.

---

1 See Article 22 Europol Council Decision

2 COM (2013)535 final

3 See Article 4(7) 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(8) of the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement

(n) The definition of "the data subject's consent" differs from that in the draft Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: General Data Protection Regulation). In view of the need to align the regulation with the principles in the data protection package presently being discussed[1], the JSB suggests that there should be no deviation from the definition used in the General Data Protection **Regulation. The regulation limits the concept of consent to a "transfer of data with data subject's consent" in Article 37(6) dealing with the time limits of the storage. Furthermore, Recital 29 refers to "transmission to third parties with the data subject's consent", which is not correct and should thus be deleted.**

Article 3, objectives

A clear description of Europol's objectives is essential for embedding its activities in a framework. Objectives define the purposes for the existence of Europol and all of its activities must be directly related to them. The core objective of the Europol Council Decision and of the regulation is that Europol must support and strengthen action by the competent authorities of the Member States when linked to specific crime.

When compared with the present objective of Europol, the description of its new objectives in the regulation may create confusion, which should be prevented from an operational and data protection point of view. Significantly, the Europol Council Decision links Europol's objective to support Member States to the organised crime, terrorism and other forms of serious crime listed in the Annex and affecting two or more Member States in such a way as to require a common approach by the Member States owing to the scale, significance and consequences of the offences.

[1] See Chapter 2 of Opinion 13/31

The regulation introduces a distinction between serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy as specified in Annex 1. The regulation apparently links the need for a common approach with the common interest by a Union policy. This may limit the competence of Europol in those cases where there is no - or no explicit - Union policy[1]. On the other hand, since there is no definition of what is to be considered as serious crime, Europol's competence may be enlarged as long as the crime affects two or more Member States. The experience of the JSB in its annual inspections, and especially the inspections of the Europol Information System, has demonstrated that without strict criteria for Europol's competence and clear definitions, there is in practice almost no limit to data processing at Europol. In the end, this may lead to great uncertainties for Member States and for Europol as to what data may be processed and under which conditions. From an operational and data protection point of view, such uncertainty should be prevented.

In view of this uncertainty, combined with the introduction of an obligation for Member States to send information to Europol and in view of the consequences of the close link between Europol's objectives and Europol's tasks as described in Article 4 of the regulation, the JSB strongly suggests redrafting Europol's objectives taking into account the comments made.

A second remark concerns the parties involved in Europol's objectives: the Member States. The evolution of Europol's work clearly demonstrates that it involves more and more law enforcement activities of third parties including private parties.

One example is the use of the Secure Information Exchange Network Application (SIENA) to exchange information between Europol and Member States, between Member States and between Member States and third parties with which Europol has concluded operational or strategic agreements. As already described in the first opinion on the regulation[2], all messages exchanged with SIENA are processed by Europol even when Europol is not the addressee of the message. Since SIENA is available to specific third parties there is a strong pressure to also use SIENA as an instrument of information exchange between Member States and those third parties and even between the third parties themselves.

---

1 See also comment in Chapter 3 of Opinion 13/31

2 §See Chapter 4 of Opinion 13/31

The JSB can understand the benefits of using a system like SIENA as a channel for exchanging information in the area of law enforcement and supports its use in implementing effective data protection provisions. However, the role of Europol in offering SIENA as an exchange tool and the processing of all data exchanged should be in line with Europol's objective: to strengthen the action of Member States in relation to specific crimes. Doubts may be raised as to whether the use of SIENA between Member States and third parties will always fall within the framework set out in Article 3. This is especially the case when the information exchanged is not related to crimes for which Europol is competent. There is no doubt that the use of SIENA for information exchange between third parties, even when it involves crime for which Europol might be competent, is not covered by the present or the proposed new legal framework, because it cannot be linked to Europol's core objective: to enhance Member States' action.

Using a messaging system such as SIENA as an instrument of law enforcement cooperation with participants outside the European Union and with a scope wider than described in the existing legal basis and in the proposed regulation can only be justified when the objectives of Article 3 are amended to provide for such a legal basis.

A clear legal basis for using SIENA (Europol's messaging service) now or in the future must be included in this regulation if its use is considered necessary for the fulfilment of Europol's objectives and tasks. Furthermore, appropriate data protection safeguards must be put in place.

Another example illustrating the need to re-assess Article 3 is the creation of the European Cyber Crime Centre EC3 and the developments in its activities. Its mandate involves engagement with international law enforcement authorities, the private sector and civil society organisations[1].

[1] Communication from the Commission to the Council and the European Parliament "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre" endorsed by the Council on 7 June 2012

Although a European Cyber Crime Centre, it is to be expected that in view of the crime involved, the activities of EC3 will most probably not stay limited to the European Union. It will thus be important to assess whether the objectives of Europol should also include certain activities related to the types of crime for which Europol is competent but which are not necessarily related to supporting and strengthening the action of Member States. If the activities as described are deemed a necessary element of Europol's future work, the objectives of Europol should also provide for a framework in which such activities may take place. The present text is not sufficient to encompass all these (future) activities. There is a clear need to introduce specific rules and effective guarantees for an accountable organisation for such activities as well.

Finally, the JSB would refer to its comments on Europol's role as described in the Terrorist Finance Tracking Programme (TFTP) Agreement[1]. That role is not connected to Europol's stated objectives. Although Member States might benefit from the processing of data by the US Treasury under the TFTP, the verification activities performed by Europol serve a purpose other than those described in its objectives.
Also, in view of possible future developments, Article 3 should contain a provision allowing Europol to fulfil other tasks it is given by international agreements, provided that these tasks are within its objectives and that its data processing is in accordance with the data protection provisions.

These comments are based on future developments to Europol's activities. The JSB has no objections against these developments in principle, but would warn that maintaining the present description of Article 3 will not permit further development of the activities referred to.

The JSB suggests re-assessing and amending Article 3 in such a way that Europol's objectives better fit its present and expected future role.

[1] See comment in Chapter 4 of Opinion 13/31

Article 4, tasks

To fulfil its objectives, Europol has to execute certain tasks. Article 4 sums up the various tasks Europol has to perform. The JSB would emphasise that such tasks should result directly from the objectives as defined in Article 3.

The present text of Article 3 does not allow for Europol to fulfil its role as an IT service provider for message exchanges in those situations where it is not the recipient of the message. The JSB refers to the comments in its first opinion and its comments on Article 3.

Without defining Europol's task as service provider and a direct relationship to its objectives in the regulation there is - except for the exchange directly related to Europol's present tasks involving Member States activities - no legal basis for what Europol and the Member States intend to do with SIENA.

As already stated, Europol processes all data exchanged with SIENA even when the data is not sent to Europol to fulfil its tasks. The description of Europol's tasks under the present legal basis and under the proposed regulation is not sufficient to cover all Europol's activities as service provider for the use of SIENA.

The JSB stresses that Europol's activities also require specific arrangements concerning the responsibilities for the data processed. What are the consequences of Europol processing data that is exchanged between Member States or with a third party when a data subject requests access to these data or contests these data? Will it be solely a Europol responsibility or are the Member States (also) responsible for handling these requests? And under which jurisdiction and applicable rules shall a decision be made when a request is made directly to a national court?

The JSB urges that a specific task be introduced for Europol to act as service provider for information exchange systems that may enhance mutual cooperation within the European Union and even beyond (provided that Europol's objectives so allow). The consequences of such a specific task should be further detailed in the articles dealing with responsibility for data and other aspects of data protection such as the right of access and retention periods.

In this respect it is also worth noting that, although the development of a communication platform for EC3 is still under development, similar issues to those concerning SIENA also need to be solved for EC3.

The comments made above clearly demonstrate that cooperation with or via Europol may often relate to action by Member States in which it is only involved as a service provider for the exchange of messages. This is one of the reasons why the JSB does not support data protection supervision solely by the European Data Protection Supervisor (EDPS), as already stated in the first opinion. In the two scenarios described above (SIENA and EC3), purely national data processed by Europol will be subject to data protection supervision by a European supervisor in view of the technologies used.[1]

Article 4(1)(a)

In line with the comments made on Article 2(b), it should be made clear that the definition in Article 2 refers to Europol's task of analysing data. This will also be crucial in distinguishing between the purposes of processing activities as defined in Article 24 of the regulation and especially between cross-checking activities (which could easily be understood as data analysis as now described in Article 2(b)) and strategic, thematic or operational analyses.

Article 4(1)(b)

When compared to Article 5(1)(b) of the Europol Council Decision, the regulation does not specify how the obligation to notify a Member State has to be complied with and whether it will involve the national units. The JSB refers to its comments on Article 7 of the regulation, dealing with Member States' cooperation with Europol and the role of the national units.

1 See in this respect Chapter 7 Opinion 13/31

Article 4(1)(c)

Here, one of Europol's tasks is described as to coordinate, organise and implement investigative and operational action. This can be either in investigations already started by Member States or as a result of a request from Europol to a Member State to initiate a criminal investigation. Furthermore, this task could also take place in the context of joint investigative teams. In line with comments already made by the JSB in its first opinion[1], the legal framework in which Europol may perform this task should be made explicit. Since these activities may be subject to a national judicial assessment of their legality, it should be made clear in a separate provision in the regulation under whose responsibility they take place and the consequences for the data protection responsibilities for data processed pursuant to such activities.

Article 4(1)(d)

The regulation presents Europol's task to participate in joint investigations teams as well as to propose that they are set up. Suggesting that a joint investigation team is set up is new compared to the Europol Council Decision and is part of the drive to extend Europol's role. What is worrying is that the data protection consequences of Europol's participation are no longer regulated. The Europol Council Decision provides for specific rules on Europol's activities when processing data in the framework of its participation in joint investigation teams. These rules cover the dissemination of data processed in Europol's files to the participants of such teams and the processing by Europol of data received in the course of such investigations. An important reason for introducing such rules in the Europol Council Decision was the experience in the past of Europol's support to Member States' investigations projects[2] that took place outside the legal framework of Europol leading to an uncontrolled form of data processing. It is important for all participants in joint investigation teams to have clear rules on the operational and data protection aspects of Europol's participation. The JSB strongly suggests introducing a provision similar to Article 6(4) and (5) of the Europol Council Decision making explicit under which legal framework Europol's data processing activities in joint investigation teams take place.

Article 4(1)(j-k)

Referring to the comments made by the JSB in its first opinion[1], these paragraphs should be deleted and the subject should be further regulated in line with Europol's objectives in Chapter VI of the regulation.

---

1 See in this respect Chapters 3 and 4, Opinion 13/31

2 Member States Operational Projects with Europol Support (MSOPES)

Article 5, participation in joint investigation teams

Referring to its comments above, the JSB strongly suggests introducing specific rules on Europol's data processing activities and responsibilities when participating in joint investigation teams.

Article 7, Member States' cooperation with Europol

Article 7(1)

This Article introduces an obligation for Member States to cooperate with Europol.

In view of the wide range of Europol's extended competences, discussions might be expected on the extent of the obligation of Article 7(1) and the consequences for Europol's data processing activities. From a data protection perspective this aspect is of importance since it is closely related to the responsibilities and controllability of data processing.

In this respect, the JSB reiterates the comments made in Chapters 3 and 4 of Opinion 13/31, dealing with Europol's role, responsibilities and tasks. An obligation to cooperate should always be accompanied by clear provisions on Europol's tasks, its role linked to national investigative and/or judicial proceedings and a clear description of the crimes for which Europol is competent.

Article 7(2 and 4)

Both paragraphs describe the establishment of a national unit in each Member State as the liaison body between Europol and that Member State and the possibility for Europol to have direct contacts with competent authorities in the Member States. The question of whether Europol may have direct contacts with competent authorities has been dealt with on many occasions. When the Europol Convention was signed, such contacts were not allowed. By Council Act of 27 November 2003[2], Article 4(2) of the Europol Convention was amended: Member States could allow direct contacts between Europol and designated authorities subject to conditions determined by Member States including prior involvement of the national unit. Furthermore, the national unit should be informed without delay by Europol. The same provision was introduced into the Europol Council Decision.

---

1 See in this respect Chapter 4 Opinion 13/31

2 Council Act of 27 November 2003 drawing up, on the basis of Article 43(1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol amending that Convention; OJ C 2, 6.1.2004, p.4

The difference with the present arrangement is that it is not the National Unit of the Member State or even the Member State itself in charge of designating with which competent authorities and under which conditions Europol may have direct contacts. Since no further arrangements are provided for in the regulation, it must be assumed that it is down to the discretion of Europol whether it intends to have direct contact with a specific competent authority. In view of the obligation to cooperate with Europol (Article 7(1) of the regulation), and taking into account that the proposed definition of a competent authority is not limited to public authorities, the JSB wonders how a national check on the permissibility of the data transfer to Europol will take place. Informing a national unit afterwards cannot be regarded as a sufficient check.

With regard to the exchange of information between a Member State and Europol, the questions of which data should be transmitted and whether it should be directed via a national unit or directly are important for establishing conditions on national level to ensure the lawfulness and quality of the personal data transmitted to Europol. It will be important to assess whether the allocation of responsibilities for Europol and the Member States (see Article 41 of the regulation) is based on a reality in which Europol and/or the Member States can be held responsible. Over the many years of supervising Europol, it has become apparent that for example the use of specific IT structures by Member States to transmit large amounts of data to Europol[1] needs to be accompanied by strict procedures for control and allocation of responsibilities within the Member States[2]. This situation will be no different when dealing with the transmission of data via SIENA to analytical work files, whether or not these files will be defined as such in the new legal basis.

The JSB suggests introducing a provision to allow Member States to set strict conditions for the direct contact between Europol and competent authorities. Such provisions should include measures ensuring the quality of the data to be transmitted to Europol (see Article 41(2) of the regulation) and could be linked to the tasks of national units. The JSB notes that Article 8(1) of Council Framework Decision 2008/977/JHA[3] on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters introduces a specific obligation to verify the quality of personal data before they are transmitted or made available.

---

1 The use of automatic data loaders to transmit data to the Europol information system

2 See JSB survey 12/61 on conditions for National Units, available at http://europoljsb.consilium.europa.eu/about.aspx

3 OJ L 350, 30.12.2008, p.60

In view of the discussions on a European Information Exchange Model, the possible use of SIENA in this model and the establishment of operational Single Points of Contact (SPOC), the JSB urges that it be clarified whether Europol national units will have a specific role in this model, and if so which, when exchanging information with Europol.

Article 7(5)

The JSB refers to its assessment of Europol's role in its first opinion.[1] In Article 7(5)(a), the regulation introduces an obligation for Member States to transmit to Europol all information necessary for it to fulfil its objectives. This includes data on crime considered a priority by the Union and a copy of all bilateral or multilateral exchanges with other Member States, in so far as the exchange refers to an offence or criminal activities falling under Europol's objectives.

Whether something is necessary for Europol is dependant on whether the data should be processed according to the purposes as defined in Article 24 of the regulation. Merely sending data to Europol without a specific purpose would not be in compliance with the basic data protection principle of purpose limitation.

Furthermore and as already stressed by the JSB in its first opinion, Europol's objectives are very broadly defined and, as a result, may cover nearly all criminal activities. This might lead to a situation where there is hardly any limit to the data to be transmitted to Europol. The possibility of competent authorities transmitting these data without involving the national unit will only contribute to the difficulties Member States may experience in controlling the flow of information to Europol. Since the regulation does not provide for specific rules for dealing with this flow of information, does not define the purpose for processing all that information, and does not provide instruments for data minimisation, this means that such an obligation is not justified from a data protection perspective. In particular, the suggestion that a free choice of IT structure in combination with the principle of privacy by design could provide for sufficient data protection safeguards should be regarded as inadequate.

1 See Chapter 3 of opinion 13/31

Article 14, functions of the Management Board

According to Article 44(1) of the regulation, the Management Board must appoint a Data Protection Officer. The JSB notes that such a task is not mirrored in Article 14. This seems strange since other duties to appoint certain officials are provided for in Article 14(1)(k, m-n). The JSB suggests inserting a new subparagraph into Article 14(1) describing the task of appointing a Data Protection Officer.

Article 14(1)(p)

The regulation does not provide for a specific role for the Director of Europol in deciding which data processing systems should be introduced. According to Article 14(1)(p), the Management Board must take all decisions on the establishment of Europol's internal structures. Since the regulation does not provide for another allocation of responsibilities for setting up data processing systems, the JSB wonders whether the regulation intends to allocate this full responsibility to the Management Board. Where the Europol Council Decision created clear rules on the information structure and a specific role for the Director of Europol in deciding to create new analytical working files, such structure and clear allocation of responsibilities is not present in the regulation. Having the Management Board be responsible has the advantage that all Member States stay involved in deciding on the information structures of Europol. However, such a responsibility might complicate the relationship between the Management Board and the Data Protection Officer. This officer is appointed by the Management Board to safeguard his/her independence. Furthermore, the Management Board is the authority dealing with possible non-compliance issues that cannot be solved between the Director of Europol and the Data Protection Officer. This would create a problem with possible conflicts of interests. The JSB suggests that the regulation should introduce clear rules for who is responsible for setting up data processing systems.

Article 23, sources of information

Article 23(1)(c)

The JSB wonders why there is no mention of private persons as sources of information. According to Article 33, Europol may under certain conditions retrieve information from private persons. It would be logical to include this group in Article 23(1)(c). The reference to Article 29(2) only refers to non-personal data and does not seem logical in view of the scope of Article 23: sources of information. The JSB suggests replacing Article 23(1)(c) with:

(c) by private parties in accordance with Article 32 and private persons in accordance with Article 33.

Article 23(2)

When compared with Article 23(1), the JSB notes that Europol's use of information from publicly available sources is not linked to a specific legal framework. Article 25 of the Europol Council Decision links the use of publicly available data to the data protection provisions of that Decision. The processing of data by Europol, even when retrieved from publicly available sources, is restricted to what is necessary for achieving Europol's objectives and should be compliant in particular with the general data protection principles of purpose limitation, data minimisation and effective data retention provisions.

For a better understanding of why these provisions need to be explicitly applicable, insight into how Europol conducts its activities is important.

The possibility for Europol to directly retrieve and process personal data from publicly available sources also covers information from commercial information providers. Past practice has demonstrated that Europol regularly purchases personal data (packets), for example from Dun and Bradstreet, an international commercial information provider. These data are used for some of Europol's analysing activities. Europol receives packages containing personal data on a large group of persons, most of them not necessary for the performance of Europol's task.

Europol justifies this by the fact that it is not always able to purchase data targeted to a specific person or group of persons since the identity of the person(s) involved is not known. Furthermore, a targeted request could reveal the target of their inquiry to the provider of commercial information. For tactical reasons alone this could not be revealed. This practice means that Europol also obtains extensive amounts of personal data not necessary in the performance of its tasks which will have to be deleted. The data protection provisions of the Europol Council Decision explicitly mention the principle of necessity of the processing of data for a specific purpose. Not having such a specific provision related to the collection of data from publicly available sources - where such a provision is introduced for retrieving information from other sources - may at best lead to misunderstandings and should thus be avoided.

The JSB suggests adding to Article 23(2) that such processing should at least be in accordance with the data protection provisions of the regulation and especially with Article 34.

Article 24, purposes of information processing activities

General comments.

Articles 24 and 25 mark the big difference between the approach of the Europol Council Decision and the regulation. Where the Europol Council Decision describes two specific aspects of Europol's tasks: the Europol Information System and the analytical work files, combined with the possibility of developing new data processing systems (Article 10(2))[1], Article 24 of the regulation intends to introduce flexibility not by describing any system of data collection, but by describing and thus limiting Europol's data processing to three purposes: cross-checking aimed at identifying connections between information and two forms of crime analysis.

Europol's core activities may be described as processing data for crime analysis projects and making information available for law enforcement authorities, either by having data available or by offering the possibility of cross-checking data with data it has processed. Furthermore, Europol offers services or intends to offer services where the processing of personal data cannot be regarded as cross-checking or analysis. The most striking examples are the use of SIENA, where Europol acts as service provider, and its verification role based on the TFTP Agreement. Examples of planned future services include publishing a list on Europol's website of the so-called "most wanted" and providing support in joint cross border operations, the European Tracking Solution. Both initiatives would be possible under the present legal basis[1] but not under the regime of the proposed regulation since they do not involve cross-checking or analysis activities. Focusing and limiting Europol's data processing activities to those referred to in Article 24 will thus not lead to increased flexibility for Europol to process data but to the opposite.

In its first opinion[2], the JSB already stated that there should be a flexible structure allowing Europol to fulfil a variety of tasks. Some of these tasks are made explicit in Article 4 of the regulation (e.g. Article 4(1)(e-f)), and some are described in a more general way (Article 4 (1)(a)).

From an operational as well as a data protection point of view, the execution of Europol's tasks should be transparent and imbedded in clear structures. These structures could also define what is expected from Europol in order to enhance Member States' cooperation and what should be the role and influence of the major stakeholders of Europol: the Member States.

---

1 Article 10(2) Europol Council Decision

2 See Chapter 5, Opinion 13/31

As already mentioned in the first opinion[1], controllability for contributors will be important from an operational and data protection point of view. Transparency and structure will also be important for the European Parliament and national parliaments to fulfil their roles as defined in the regulation.

Another data processing activity that is not covered by Article 24(1) is the processing of data transmitted to Europol, or retrieved by it from the sources referred to in Article 23(2), where it is not yet possible to assess whether all of these data fall under Europol's objectives. This is a problem that was already discussed and solved by amending the Europol Convention in 2003 and by the Europol Council Decision. Although the need to temporarily process data allowing Europol a certain period for assessing these data is in practice still very much required, there is no legal basis for this in the regulation anymore. The assessment activities referred to in Article 10(4) of the Europol Council Decision are not covered by the activities as defined in Article 24.

In order to create a legal basis for Europol to process and assess any incoming information if it falls within its objectives, Article 24 should include a provision similar to Article 10(4) of the Europol Council Decision.

Article 24(1)

This paragraph defines cross-checking as an activity aimed at identifying connections between information. Cross-checking has been defined as a purpose of processing separate from the other purposes of processing as referred to in Article 24(1)(b-c): analysis of a strategic or thematic nature and operational analysis in specific cases. However, the JSB notes that cross-checking is also an important activity in crime analysis: establishing connections between persons often in combination with other information (e.g. telephone numbers). Article 24(1) is thus not distinctive enough. Cross-checking activities as referred to in that Article include both processing activities as part of analytical activities and cross-checking outside the scope of processing for analysis purposes. This distinction is of great importance since a part of Europol's activities is to simply check on request of a Member State whether data provided by that State such as names, telephone numbers, IP addresses and licence plate numbers match data already processed by Europol. The purpose of such a match is to allow a Member State to decide on further activities. Such a cross-check request is in itself not a reason for further processing these data at Europol after the cross-match is finalised.

---

1 See Chapter 6, Opinion 13/31

Nor should this be permitted, since the sometimes long lists of personal data to be cross-checked often appear to concern persons not having any relation with crime or criminals and who cannot be regarded as persons belonging to the categories of persons as defined in Annex 2. There is no legal basis for any further processing of these data.

The JSB concludes that the distinction drawn between three purposes does not present the reality of the work of Europol and that Article 24(1) should be reconsidered.

Article 24(2)

The second paragraph of Article 24 describes, by referring to a specific annex (Annex 2), the categories of personal data and categories of data subjects that may be collected for each of the specific purposes referred to in paragraph 1 of that Article.

What the regulation in fact does is to copy and paste into Annex 2 various articles from the Europol Council Decision and Council Decision 2009/936/JHA adopting implementing rules for Europol analysis work files[1]. The content of the data presently processed in the Europol Information System and in the analytical work files is cumulatively presented in that Annex. By using the word "collected" the regulation implies that the aim is to process data for a longer period. This is not strange since Europol's core business as already described in the general part of the comments on Article 24 also includes the availability of personal data.

What the regulation apparently aims to do is to create the possibility of setting up a system in which data can be processed and with which Europol and Member States can cross-check data.
This conclusion seems to be justified since the data that may be collected for cross-checking purposes are exactly the same as the data to be processed in the Europol Information System. It cannot be expected either that Europol - after the implementation of the regulation - will not continue processing data in the Europol Information System as it has done until now.
The JSB stresses that the regulation limits the functioning of what is now the Europol Information System to mere cross-checking functions instead of having a central database that - as is now the case - may also be used for broader consultation purposes.

[1] OJ L 325 11.12.2009, p.14

Furthermore, the JSB notes that the regulation no longer provides for the additional safeguards and structure within which the data may be processed[1], including the possibility for Member States to directly input data into the system. It is to be expected that this will have negative consequences for the operational functioning of the system to be set up and will downgrade the level of data protection. In this respect the JSB furthermore notes that some data protection rules - such as the obligation to delete data when proceedings against a person have been dropped or if a person has been definitely acquitted - have been included in an annex to the regulation. In view of their fundamental nature, these matters should be regulated in the regulation itself instead of in an annex. The same applies to the definition of the persons whose data may be processed for each of the specified purposes: this should not be regulated in an annex.

In a similar way, the regulation describes the content of processing activities relating to the analysing purposes as defined in Article 24(1)(a-b).

The main differences between the Europol Council Decision, Council Decision 2009/936/JHA and the regulation are Europol's accountability for analytical data processing, the controllability of these activities for the contributors and transparency regarding what specific analysis projects are executed. The present robust regime for Europol's analytical activities provides for specific rules defining Europol's and Member States' roles when participating in specific projects[2] and the influence and control they have over the use of the data processed for such projects. This accountability and controllability have always been regarded as essential elements for creating trust when sharing operational information and the processing of that information via a common platform such as Europol. They also created transparency for the Member States and Europol's staff, specifying the details of a project including the participants. There are specific provisions safeguarding this in Article 14(5), (7) and (8) of the Europol Council Decision and in numerous Articles in Council Decision 2009/936/JHA[3].

---

1 See Article 13 (2-5) Europol Council Decision

2 The JSB uses the term "project" for all activities in one of the two analytical work files either in a focal point or target group.

3 See especially Article 3(2)(3); Article 4(2);Article 5; Article 7(3);Article 8; Article 9;Article 10; Article 17

Based on its extensive experience of the evolution of Europol's working methods and especially with the practical aspects of crime analysis, the JSB does not expect that the way Europol performs crime analysis will change in the coming decade. It will remain necessary to have specific analysis projects for investigations into specific forms of crime and into single- or multi-commodity criminal organisations. Furthermore, the specific counter-terrorism data processing activities will also remain part of Europol's core activities. All these activities can only be effective and governed by an effective data protection regime when all possibilities, roles and responsibilities are transparent for all involved.

Not having such provisions anymore diminishes the necessary trust and may very well put operational participation in analytical processes at risk. It will also create a situation where the different responsibilities and data protection requirements are no longer sufficiently defined. In this respect, the JSB wonders why, in the part of Annex 2 dealing with Article 24(1)(a), the regulation copies the instruction of Article 12(5) of the Europol Council Decision regarding the effect of decisions in judicial proceedings, while no longer using the similar but more tailor-made instruction of Article 7(3) of Council Decision 2009/936/JHA in relation to the analytical activities referred to in Article 24(1)(a-b) of the regulation.

Article 25, determination of the purpose of information processing activities

Article 25(1)
Article 25 obliges Member States, Union bodies, third countries and international organisations providing information to Europol to determine the purpose for processing as defined in Article 24(1).

In general, the JSB supports such an obligation and also welcomes the provision allowing the processing of information for another purpose only if authorised by the data provider.
The JSB stresses that any determination of a purpose cannot be done in the same general terms as in Article 24(1). According to the principle of purpose limitation the purpose should be specific. The purpose of "data analysis" is too broad and makes it impossible to assess which data can be considered as necessary for the purpose of Europol's analysing activities.

However, and in connection with its advice on Article 24, the JSB fears that the way the regulation links the purpose of processing with Europol's processing activities may lead to a situation where the practical implementation of Article 25(1) becomes problematic.
Presently, Europol performs crime analysis in 25 so-called focal points, most of them also facilitating operational analysis for certain Member States in a great number of specific investigations (target groups). Past practice has demonstrated that these focal points can only be effective when a data collection plan is in place and when the participating Member States commit themselves to transmitting the data in conformity with the collection plan. Transparency of the existence of such focal points and the collection plans is thus essential for Europol to be effective and for Member States to cooperate. As already highlighted in the comments on Article 24(2), the regulation does not ensure the transparency of the type of processing activities performed in accordance with this Article.
A consequence of Article 24 in combination with Article 25(1) is that it might thus be difficult for a contributing Member State, third state or other to describe precisely the purpose for which it is sending data to Europol and for which specific recipient within Europol (specific analysis project or other specific activities) the data are intended. This will undermine the protection offered by applying the purpose limitation principle, e.g. which data are necessary. It may also create operational problems. This will especially be the case when the authorities transmitting data to Europol have no structured relationship with that organisation and may not be aware of the (specific) analysis projects Europol and Member States are involved with.

As the JSB already advised in its assessment of Article 7(4) of the regulation, there is a clear need to introduce conditions for sending information to Europol. Such conditions may help Member States in defining the purpose for which they send data to Europol.

The JSB would also repeat what it advised when assessing Article 24(1): cross-checking is also an important activity in crime analysis: establishing connections between persons often in combination with other information. Under the Europol Council Decision, Europol - after consultation with the JSB - developed a new analytical concept[1] including cross-matching to prevent double processing and to establish links necessary for the analytical process. Such cross-matching is automated and executed on a daily basis. The JSB wonders whether this practice could continue under the regulation. Cross-checking is defined as a separate purpose, distinguishing it from analytical processing activities.

In view of the comments made above, the JSB strongly suggests that it be reconsidered whether Articles 24 and 25 - in combination with the other provisions in the regulation - provide for a structure in which Europol can effectively fulfil its task in a flexible way and in which the necessary elements of controllability are imbedded. The JSB assessment is that Articles 24 and 25 of the regulation will limit Europol's activities compared to what is possible under the present legal basis. Under the regulation, Europol cannot use SIENA and it will not be possible either to develop new data processing activities in which cross-checking and the forms of analysis as referred to in Article 24 will not play a role. Furthermore, as already noted by all European Data Protection Authorities[2], eliminating the existing Europol systems and files will result in the removal of system-specific safeguards, which will lower the existing level of data protection.

The JSB warns that there is a clear risk that the proposed regulation will not enable Europol to fulfil its main task of strengthening mutual cooperation between Member States and other parties in the best possible way where operational interest and data protection are in balance. The JSB suggests assessing whether the present structure could be improved and where necessary made even more flexible. For example, the prohibition of the processing of sensitive data in Article 10(2) of the Europol Council Decision could be deleted. Such processing could be allowed under the same conditions as for Europol's other systems.

---

1 See Chapter 5, Opinion 13/31. The new analytical concept was launched in June 2012.

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

Article 26, access by Member States and Europol's staff to information stored by Europol

Article 26(1) and (2) replaces Article 15 of the Europol Council Decision that describes the index function on Europol's analysis files. It introduces the possibility for Member States to check whether data on a specific person is processed in the analytical work files (Europol Council Decision) or in the analytical activities (regulation). When searching data through the index function or via the hit/no hit system, personal data (information that data on a specific person is processed by Europol) is presented to the requesting party. The JSB suggests deleting the word "indirect".

Article 27, access to Europol information for Eurojust and OLAF

Article 27 regulates access to Europol information for Eurojust and OLAF.
In view of the close relationship between Europol's and Eurojust's activities and the crime areas defined as part of their objectives and tasks[1], the JSB understands the logic in allowing access to each others' information. On 17 July 2013, the Commission presented a proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust). Article 40(1) of the draft Eurojust regulation mirrors Article 27(2) of the regulation.

As a first remark, the JSB would repeat what it already advised on Article 26. Access on the basis of a hit/no hit system is not "indirect" access. The JSB suggests deleting the word "indirect".

Access should be granted only for the tasks of the organisation allowed such access and should only cover data processed that fall within the objective/task of the accessing organisation. There should thus be a close relationship between the data to be accessed and the organisation having such access. As already stated above, there is a close relationship between Europol and Eurojust tasks and their fields of operation.

1 Article 3 of the regulation and Article 2(1) of the proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust), COM(2013)535, 17.7.2013

The JSB notes in this respect that Eurojust has the same access rights as Member States: access to all information processed for the purposes of Article 24(1)(a-b) and via a hit/no hit access to data processed for the purposes of Article 24(1)(c). It is interesting to note that the proposed Eurojust Regulation limits Europol's access to Eurojust's data processing system to a hit/no hit access although the data processed are almost identical as for the purposes of Article 24(1)(a-b).

Another aspect that requires attention is the need to inform each other when after consultation of each other's data there are indications that data may be incorrect or conflicting with other data. It is in the benefit of both organisations that an obligation to inform each other is introduced.

The JSB wonders whether OLAF's tasks and competences cover the same area as Europol's objectives. As already stated above, access should only be allowed for data processed that fall within the objective/task of the accessing organisation. The JSB doubts whether this is the case with OLAF. Although there might be a certain overlap between the objectives of Europol and OLAF, a consequence of Article 27 is that OLAF has access to what is probably a huge amount of personal data that do not have any link with its tasks and competences. This is not acceptable from a data protection point of view. The JSB suggests reassessing OLAF's access to Europol's data processing activities. If access is considered necessary and important, Article 27 should contain an instruction for Europol to introduce technical measures ensuring that only data that fall under OLAF's competence can be accessed.

Article 29, common provisions

Article 29(1-3)

Article 29 creates the general legal basis for the exchange of information between Europol and its partners. More detailed provisions are provided for in Articles 30-33.

Paragraph 1 describes who Europol's partners are; paragraph 2 allows Europol to exchange directly all information - except personal data - with these partners and paragraph 3 describes that Europol may receive and process personal data from these partners except from private parties in so far as necessary for the performance of its task and subject to the provisions of this Chapter.

In view of the function of Article 29: describing the common provisions for Europol's relations with partners, the JSB notes that paragraph 3 excludes private parties as a source of information. According to paragraph 1, private parties may be of such importance for Europol that they are recognised as possible partners for it[1]. Not including those third parties in paragraph 3 may lead to confusion that should be avoided. In this respect the JSB notes that any exchange as referred to in paragraph 3 is also subject to the other provisions of Chapter VI, which include special conditions when receiving information from private parties.

Article 29(3)

The JSB suggests not deviating from the text of the Europol Council Decision when not necessary. The JSB refers to the condition in the Europol Council Decision that links the receipt and processing of data to the legitimate performance of Europol's task[2].

Article 29(4)

This paragraph contains common provisions for transmitting data by Europol to the partners referred to in it. Here the regulation follows the same structure as in the Europol Council Decision: personal data may only be transmitted by Europol to the partners as referred to in paragraph 1 with the exception of third parties. The JSB in general supports excluding third parties as recipients of

---

1 This might especially be the case for EC3.

2 See Articles 22(3) and 23 (4) of the Europol Council Decision

personal data processed by Europol. However, the JSB notes that in certain crime areas - e.g. cyber crime - such an exchange might be expected; asking a service provider to provide traffic data related to a specific IP address is already regarded as transmitting personal data (even if the identity is not known yet) to that third party. In view of the increasing attention to cybercrime in the European Union (e.g. the creation of the European Cybercrime Centre at Europol), the JSB could understand that providing for a limited and strictly conditioned possibility to exchange information with specific third parties can be balanced with data protection interests. The JSB further refers to what it advised in this opinion on EC3 and Article 3 of the regulation.

Another aspect that needs further attention is the obligation for Europol to transfer data only with the consent of the Member State that provided the data. Europol should seek that consent unless the providing Member State has granted its prior authorisation either in general terms or subject to specific conditions. This system is used in the Europol Council Decision. The regulation now introduces an additional rule: when a Member State that provided data to Europol did not expressly limit the possibility for transfer, its authorisation may be assumed. This changes the burden of proof as to whether Europol is allowed to transmit data to its external partners. The JSB fears that such a wide exemption will create the risk that all data sent to Europol without an explicit and strict prohibition for transmission may thus be available for transmission to Europol's partners. Especially data sent to Europol for simple cross-checking or the copies of bilateral or multilateral exchanges[1] will not be labelled prohibiting their onward transfer. At least, Member States or their partners in the bilateral or multilateral exchange will not be aware that what is exchanged will be available for transmission to Europol's partners unless they explicitly prohibit this. In view of the data protection implications of such an approach, the JSB urges that such risks be prevented and that the rule that Member State's consent is the basic prerequisite be maintained.

[1] See Article 7(5)(a) of the regulation

Article 29(5)

This paragraph allows onward transmission by Member States, Union bodies, third countries and international organisations. The JSB notes that Council Decision 2009/934/JHA, adopting the implementing rules governing Europol's relations with partners, including the exchange of personal information[1], also contains specific provisions (Article 18(2) and (3)) regarding the need for consent for onward transmission. The obligatory consent of Member States for onward transmission by a Europol partner of information provided by that Member State is not carried over into the regulation. The JSB notes that the regulation has also not carried over the specific safeguards introduced in Council Decision 2009/934/JHA in relation to onward transmission (e.g. Article 18). There are no specific conditions formulated under which Europol could give its consent. The JSB stresses that not maintaining the safeguards of Council Decision 2009/934/JHA will unacceptably lower the level of data protection in relation to onward transmission.

Another issue that needs further attention is the question of whether Europol would be allowed to consent to onward transmission to a third state if Europol would not be allowed to exchange information with that third state based on Article 31 of the regulation. The JSB suggests introducing more conditions for Europol to consent to onward transmission using the relevant articles of Council Decision 2009/934/JHA as an example.

[1] OJ L 325, 11.12.2009, p.6

Article 30, transfer of personal data to Union bodies

Article 30 creates the legal basis for transferring personal data to Union bodies. As already stated in its comments on Article 2(c), the JSB notes that the general concept of what may be understood as a Union body has been enlarged to include missions and entities. The JSB assumes that this has been done to create a legal basis for transmitting Europol data to European Union police missions and the European Union Rule of Law mission[1]. The JSB welcomes the solution found allowing Europol - under the conditions of the regulation - to provide information to these missions. However, and as already stated in its first opinion[2], it is common practice for these missions in the execution of their tasks to share data (and thus also data transmitted by Europol) with the authorities of third states. In line with what the JSB already advised on Article 29(5), the regulation lacks a provision that sets out sufficient conditions for such further transfers. Without such provision, the onward transmission between Union bodies and with third parties lacks sufficient safeguards.

Article 31, transfer of personal data to third countries and international organisations

Article 31(1)
Article 31 provides for specific rules for the transfer of personal data to third countries and international organisations.
The JSB welcomes the introduction of the adequacy decision streamlining this procedure with the data protection package presently being discussed.

When an adequacy decision is made or an international agreement as referred to under (b) is concluded, Europol may conclude working arrangements to implement such adequacy decisions or agreements. The regulation does not provide for further conditions to be taken into account when concluding such working arrangements. Without such further conditions, the strict data protection regime and effective measures as included in the Europol Council Decision and its implementing

[1] See point 4.3.1 of The Stockholm Programme- an open and secure Europe serving and protecting citizens OJ C115, 4.5.2010, p.1
[2] See Chapter 4 of Opinion 13/31

acts are not maintained. The JSB urges that such rules be introduced, either in the regulation or in separate rules to be adopted by the Management Board in consultation with the external data protection supervisor. Such strict rules should at least include rules on onward transmission in the recipient third state or international organisation, the retention periods, the correction or deletion of data and rules concerning the transmission of sensitive data.

What should also be taken into account when transferring data to third states and international organisations is under which conditions such a transfer should be allowed. One of the data protection safeguards introduced in Council Decision 2009/934/JHA is the limitation of such transfers to when necessary in individual cases. Article 31(1) as it stands would open up the possibility of sharing data without such assessment and thus not preventing that data will be provided for more general law enforcement purposes.
The JSB underlines that it is necessary to introduce further and more specific rules for Europol when concluding the working arrangements as referred to in Article 31(1).

When a relationship with a third party or international organisation is in place in compliance with Article 31(1), transfers to third states and international organisations need no further authorisation. This provision diminishes any form of control over what will be transmitted. In addition to the advice already given in relation to Article 29, such a lack of control also includes a lack of reasoning by third states as to why they need the data. The rule should be that where there is insufficient motivation no authorisation is granted. The JSB notes that Article 15 of Council Decision 2009/934/JHA contains an obligation for the requesting third state or international organisation to indicate the purpose and the reason for which it is requesting the data. Without such an indication no data will be transferred.
The JSB stresses that there is no reason for not continuing the present system and that the regulation should not undermine - as it does now - the controllability of data to be transferred to third states and international organisations.

It would also create a strange situation if data to be transferred in accordance with Article 31(1)(c) were to be conditioned with these effective operational and data protection provisions and transfers based on Article 31(a-b) were not.

In accordance with the need to control the transmission of data to third parties and international organisations, Europol should be obliged to keep records of all transmissions of data under this Chapter and of the grounds for such transmission[1]. Such an obligation is not limited to the transmissions based on Article 31 but should cover all transmissions to Europol's partners as referred to in Chapter VI. The provision of Article 43 on logging and documentation is not sufficient to create the level of controllability and accountability needed.

Article 31(2)

This paragraph introduces derogations from the rules of paragraph 1. Such derogations are logical in view of the work of Europol. The JSB notes that the regulation has copied the grounds for a derogation from the Europol Council Decision and added two reasons for derogation that are presented in Article 36 of the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement.

The JSB welcomes the fact that it has been made explicit that a decision based on this paragraph should always be on a case-by-case basis. Without this condition, the nature of the decisions made according to Article 31(2) cannot be categorised as derogation.

The JSB regrets however that the regulation does not make provision in Article 31(2) for considerations to ensure the interests at stake and data protection are balanced[2]. Even when the interests at stake are high, data protection issues should also be taken into account. The JSB notes that in the very few specific cases where Europol used the possibilities to derogate from the general rule, it was able to make a careful data protection assessment before deciding on the transfer.

Article 31(2) also opens up the possibility that the Management Board, in agreement with its external supervisor, may authorise sets of transfers in conformity with the reasons for derogation as defined in Article 31(2)(a-d). When assessing this possibility, the existence of safeguards with respect to the protection of privacy and fundamental rights and freedom of individuals should be taken into account.

The JSB supports in general such provision though it warns that the use of this possibility should remain limited to derogation from the standard rule. In view of this, it should be made clear that the authorisation of the Management Board can only be given on a case-by-case basis.

---

1 See Article 10 Council Decision 2009/934/JHA

2 See Article 23(8) Europol Council Decision

Article 34, general data protection principles

The JSB welcomes the introduction of the general data protection principles. These are of course not new and are based on the principles already applicable to Europol. In view of the introduction of a new data protection framework based on Article 16(2) of the Treaty on the Functioning of the European Union, the JSB highlights that the basic data protection principles underlying the regulation should be consistent with that framework. The Article 29 Working Party already called for such consistency in its opinion on the data protection reform package[1]. It specifically called for consistency between the principles relating to personal data processing and urged that Article 4 of the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement be streamlined with Article 5 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. A similar issue arises with Article 34(d) of the regulation, in which the obligation to have data kept up to date only applies "where necessary". The main idea of the principle of Article 34(d) is that the data should always be accurate and kept up to date, not only when it is deemed necessary.

Article 35, different degrees of accuracy and reliability of personal data

Article 35 describes the different degrees of accuracy and reliability of personal data. It is copied from Article 12 of Council Decision 2009/936/JHA: the implementing rules for Europol analysis work files. By introducing these degrees of accuracy and reliability into the regulation, the obligation for such assessment applies to all data to be sent to Europol and processed by Europol. In this respect the JSB notes that the regulation did not copy the obligation for Europol to assess the results of its analysis activities in accordance with Article 35. Since Europol is to be held responsible for the results of the analysis, a responsibility which is further made explicit in Article 41 of the regulation[2], and in view of the importance of being able to assess the result of the analysis, especially in specific investigations, Europol should be held responsible for making such an assessment in accordance with Article 35. The reliability of analysis results should always be known by the recipients of those results.

---

1 Opinion 01/2012 of the Article 29 Working Party

2 See in this respect also Article 29(1)(b) last sentence of the Europol Council Decision: Europol is responsible for data resulting from analyses conducted by it.

Article 36, processing of special categories of personal data and of different categories of data subjects

Article 36(4)

The JSB highlights that any decision based on the provision of Article 36(4) is the responsibility of the controller – Europol. This should never become a responsibility for the external supervisor. The JSB furthermore stresses that the conditions to be complied with in Article 36 only underline the need for transparency and structure allowing Member States to carefully assess whether they should transmit data as referred to in Article 36 to Europol.

Article 36(6)

The JSB does not support the obligation to provide an overview of the data as referred to in Article 36(2). It creates an unnecessary transmission of sensitive data that cannot be effectively assessed by the external supervisor without the context in which the data are processed. The JSB suggests limiting this obligation to having such an overview available at Europol.

Article 37, time-limits for the storage and erasure of personal data

Article 37(4)

Article 37(4) opens up the possibility for Member States to indicate at the time of transferring data to Europol a specific retention time, shorter than the three year review period. The JSB welcomes such a specific provision solving an existing practical issue, since it clarifies Europol's and Member States' responsibilities in these situations.

Such limitations of the retention period are often based on restrictions imposed by national law when processing specific data or data relating to specific categories of persons. The JSB refers to what it stated in its first opinion: "Europol is only allowed to process data when Member States are allowed to process these data"[1]. Also, in view of the national judicial scrutiny, it is logical that Article 37(4) links the further processing by Europol to the authorisation of the providing Member State.

Article 37(5)

Article 37(5) introduces a similar procedure for situations where data are deleted on national level based on the normal national retention periods, or when data are deemed not necessary anymore, or incorrect, or when a person is acquitted of all charges[2]. It copies Article 20(3) of the Europol Council Decision and relates to another reason for having data deleted before the three year review of Article 37(2) of the regulation. This explains the difference between the need to have authorisation as required by Article 37(4) and informing the Member State in accordance with Article 37(5).

Article 37(6)

This paragraph defines the exemptions from the obligation to erase data. The reasons for applying exemptions are either in the interest of the data subject (points a, b and d) or for purposes of keeping proof (point c).

The JSB welcomes[3] the clear definition of these exemptions. However, and in addition to what is already stated in the comments on Article 24, the further processing of these data for the specific purposes of the exemptions cannot take place in view of the exhaustive enumeration of purposes for processing as defined in Article 24: cross-checking and analysis.

---

1 See Chapter 3, Opinion 13/31

2 See also JSB comments on Article 24(2)

3 See also JSB letter 12/69 of 18 October 2012 to the Commission asking for special protection for data subjects when involved in a proceeding against Europol, available at http://europoljsb.consilium.europa.eu/about.aspx

The JSB repeats its call to reconsider Articles 24 and 25 and also to provide for a legal basis for the further processing of personal data for the reasons defined in Article 37(6).

The exemptions in Article 37(6) will also have their consequences for the way Europol operates. For example, linking the use of data to the consent of the data subject (Article 37(6)(a)) must have as a consequence that those data are in fact not processed anymore in any system that is subjected to the daily cross-matching activities. The same situation might occur with the exemption in Article 37(6)(d).

In relation to the exemption in Article 37(6)(b), the JSB already advised the Commission "that the Europol Regulation should include an obligation for Europol to make - at the time an access request is made by a data subject - a copy of any data processed relating to that individual and to ensure that that copy cannot be changed. The copy should be kept until all legal procedures in which these data play a role are finalised."[1]

The JSB further notes that maintaining data for purposes of proof raises similar issues. Maintaining data may refer to the data used in analysis activities and/or to specific decisions in a criminal investigation made by Europol (e.g. Article 4(c)). It may also refer to the forensic services provided for by EC3.
The JSB underlines that Europol's increasing role may become the subject of scrutiny in national judicial proceedings. Europol is responsible for assisting Member States and even initiating and coordinating activities; all these activities might, as said before, be subject to national judicial scrutiny.

The JSB strongly suggests further considering which requirements should be in place to comply with the need to provide proof. Such requirements may differ depending on the type of activities performed by Europol (from simple logging of a search to explain how an analysis result was achieved, to demonstrating that the extracted data from a mobile phone are not compromised).

[1] See also JSB letter 12/69 of 18 October 2012

Article 38, security of processing

The JSB suggests introducing a new article dealing with the obligation for Europol to notify a personal data breach to the data protection officer and to the external data protection supervisor. This would bring more consistency with the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement.

Article 39, right of access for the data subject

Article 39 covers one of the most fundamental aspects of data protection: the right of access for a data subject. The present text is partly based on Article 12 of the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement and introduces some provisions relating to Europol's specific tasks.

Article 39(1)
The regulation apparently tries to introduce a provision dealing with how to respond to a request for access when no data are being processed by Europol. The way this is done, however, creates an inconsistency in Article 39(1) second sentence and under (a). It should not be possible to answer a data subject whose data are being processed that no data are being processed. Furthermore, such a construction could lead to confusion as to what to answer a data subject whose data are not being processed.

The right of access consists of two elements: the right to obtain information as to whether or not personal data relating to the requesting data subject are being processed and if so, the right to obtain certain information about that processing including a knowledge or a copy of what is actually being processed.
The limitations to the right of access concern both elemnet. In this way, a controller can assess whether there is an exemption applicable to the right to obtain information.

Both the Europol Council Decision and the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement contain such a specific provision. The regulation mixes the two aspects, which might result in confusion as to how to apply the right of access and, when applicable, the grounds for exemption. Such confusion should be prevented and the JSB suggests deleting Article 39(1)(a).

Since the right of access clearly includes receiving information on the data processed, a new sub a) could be introduced providing that the data subject may receive a copy of the data processed or information on what is actually being processed.

Article 39(5)

This paragraph sums up the possible exemptions from what is called "access to personal data".

As already stated on Article 39(1), the right of access consists of two aspects: the right to be informed as to whether or not data are being processed and if so, the right to obtain information about that processing.

In view of this, the exemptions thus apply to both aspects and not only to the access to personal data. In order to ensure this, the first sentence of Article 39(5) could better be replaced by: "The provision of information in response to a request under paragraph 1".

The JSB furthermore notes that the regulation also deviates from, or at least does not explicitly recognise, the principle that where an exemption is applied, it has to be demonstrated to what data it is applied. In cases where an exemption is only necessary for part of the data processed, partial access is obligatory. For this reason, Article 30(5) of the Europol Council Decision states that "…. shall be refused to the extent that such refusal is necessary…". Article 13(1) of the draft Directive on the protection of individuals with regard to the processing in the area of law enforcement makes this even more explicit: "to the extent that such partial or complete restriction constitutes…".

The JSB urges that a similar text be introduced in Article 39(5) of the regulation.

The text could read as follows: "The provision of information in response to a request under paragraph 1 shall be refused to the extent that such partial or complete refusal is necessary to:…".

Another aspect that needs attention is the following. Article 30 of the Europol Council Decision obliged Europol and the Member States to also take into account the interests of the person concerned (the data subject) when assessing the applicability of an exemption.[1] This emphasises the need to make a case by case assessment where sometimes more general law enforcement interests need to be balanced with specific individual interest. The JSB urges that this obligation be maintained in Article 39.

As a last remark, the JSB suggests introducing a provision obliging Europol to make - at the time an access request is made by a data subject - a copy of any data processed relating to that individual and to ensure that that copy cannot be changed. The copy should be kept until all legal procedures in which these data play a role are finalised (see JSB comment on Article 37(6)).

Article 40, right to rectification, erasure and blocking

Article 40(4 and 5)
These two paragraphs deal with the procedure of rectification, erasure or blocking of data provided by third countries, international organisations (Article 40(4)) or by Member States (Article 40(5)). The JSB wonders why no provision is introduced for Union bodies. Especially in view of the close relationship promoted between Europol and Eurojust and OLAF, such a provision should be evident.

Article 41, responsibility in data protection matters

Article 41 describes the data protection responsibilities for data processed by Europol. The general principles of data protection as defined in Article 34 are used to divide the different areas of responsibility.
The JSB underlines that a balanced allocation of responsibilities is crucial for Europol and the Member States. It does not only formally define these responsibilities, it also has a practical impact on the design of Europol's IT systems and the procedures that need to be in place to actually ensure compliance with these responsibilities.

[1] Article 30(5) last sentence of the Europol Council Decision

Article 41(2)

The responsibility of Member States is limited to having the data sent to Europol accurate and up to date.

For all other data processed coming from the sources referred to in Chapters V and VI of the regulation, Europol should be responsible also in the light of the consequences of such processing on the individual concerned. However, Article 41(2) excludes Europol responsibility for data transmitted to Europol and processed by Europol from private parties and private persons. The JSB wonders why no responsibility is allocated for the processing of the data coming from these sources. Europol had a responsibility for the processing of these data under the Europol Council Decision[1] and the JSB fails to see why such a responsibility is not deemed necessary anymore.

Another aspect that needs attention is that no specific mention is made of Europol's specific responsibilities regarding the results of analysis conducted by Europol[2]. The JSB understands that most aspects of this responsibility are covered by Article 41(2), but experiences with the analytical work of Europol and the subsequent products demonstrate a clear responsibility for Europol to keep the results of crime analysis accurate and up to date. In situations where, based on Member States' responsibilities to have data sent to Europol changed in case of being inaccurate or not up to date, Europol should be held responsible for ensuring that in these situations and where now amended or even deleted data were used to prepare an analysis report, that report should be amended or replaced by an updated version. The annual inspections of the JSB demonstrated that this specific responsibility is essential.

The JSB urges that this specific responsibility for Europol be reintroduced.

Article 41(4)

This paragraph describes the responsibility of Member States for the legality of transmitting data to Europol and the responsibility of Europol for the legality of transmitting data to Member States and third countries and international organisations. In its comments on Article 29(4) the JSB already raised questions on the procedure introduced to assume authorisation for transfer of data to third countries and international organisations. The JSB can support Europol's general responsibility for the legality of transfers but stresses that the way this responsibility should be ensured is dependant on how Article 29(4) will be interpreted.

---

1 See Article 29(1)(b) of the Europol Council Decision.

2 Article 29(1)(b) of the Europol Council Decision specifically defines this responsibility for Europol.

Article 41(5)

The JSB supports the introduction of a specific provision for the responsibilities linked to the transfer of data between Europol and Union bodies. The JSB only wonders why the additional and general responsibility of Europol for its data processing as explicitly recognised in Article 29(3) of the Europol Council Decision is now apparently only linked to Europol's responsibility in respect of the legality of transmission of data to Union bodies. The JSB urges that this additional responsibility, which has proven its value in the daily functioning of Europol, be included in a separate paragraph. For the same reason, the JSB advises inclusion of the explicit obligation for Europol to inform the party that has inputted data in a system used by Europol that it has evidence that the data are factually incorrect or unlawfully stored[1].

As a last remark, the JSB refers to its comments on Article 4: to introduce a specific task for Europol to act as service provider for information exchange systems. The consequences of this specific task are of importance for the allocation of the responsibilities of Europol as service provider. These responsibilities will, as far as they concern the processing of data in messages not directed to Europol but processed by Europol, be different than as presently defined in Article 41. Europol cannot be held responsible unless it has access to and influence over the processing of these messages. Since many messages are only exchanged between Member States (and/or with third countries) and not with Europol, a responsibility for the content of the messages would not be compliant with Europol's objectives. The JSB stresses that Article 41 should also include a provision dealing with Europol's responsibilities when acting as a service provider.

[1] A similar obligation is provided for by Article 29(4) of the Europol Council Decision.

Article 44, Data Protection Officer

It is very important that the function of a Data Protection Officer for Europol is maintained. Past practice has demonstrated that such an officer and his staff have a positive influence on the implementation of data protection provisions in practice. The importance of this function is underlined by having the officer appointed by the Management Board and the adoption by that board of the implementing rules concerning e.g. tasks, duties, powers and safeguards. The JSB also welcomes the obligation to provide the Data Protection Officer with sufficient staff and resources. In this respect, the JSB wonders why Article 44(11) contains a limitation on staff having access to personal data. Past practice has demonstrated that it is not always clear whether data to be assessed by the staff of the Data Protection Officer should be regarded as personal data. The JSB refers to a certain type of log files to be checked and situations in which it has to be assessed whether certain data are to be regarded as personal data. The JSB suggests better aligning the last sentence of Article 44(11) with the provisions of paragraphs 8 and 9.

A last remark concerns the use of the word "position" in Article 44(11). Such a word may possibly influence the formal imbedding of the Data Protection Officer in the organisation, which might influence his/her functioning. Since the implementation rules are to be adopted by the Management Board, it should be left to the Management Board to create the best structure for the functioning of the Data Protection Officer.

Article 45, supervision by the national supervisory authority

Logging and documentation is an essential element of control for Europol, the national supervisors and Europol's external supervisor. The JSB already uses these logs and documentation when inspecting Europol. In view of the close relationship between Europol and the Member States, the JSB supports initiatives to enhance a harmonised use of this information in auditing activities on national and Europol level.

Article 46-50

In its first opinion[1] the JSB stressed that the involvement of the national DPAs in the data protection supervision of Europol 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 for further processing and use in criminal investigations and prosecutions. Effective data protection supervision of Europol thus cannot be done without the strong involvement of the national DPAs. A similar conclusion was also drawn by the conference of European Data Protection Authorities[2].

The JSB repeats that it does not support the Commission's idea of making the EDPS solely responsible for the supervision of Europol.
Consistency in the data protection supervision of Europol is best served by combining national data protection supervisors experienced in supervising the activities of national law enforcement authorities. The extensive national experience of how to deal with law enforcement information is essential. Similar arguments concerning the specific nature of this field form the basis for Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

The comments made in this second opinion on the regulation only confirm and further support that effective Europol supervision can only be done when combining the national experiences into a strong and robust external data protection supervisor. The specific role and tasks of Europol distinguishes it from other agencies and supports the need for a more specific and specialised form of data protection supervision.

The JSB also repeats that it has also considered whether it would be an option to implement a coordinated supervision model used for Eurodac, VIS and SIS II. However, such a model may not lead to the vigorous supervisor that is needed for Europol. It should also be noted that the data protection responsibility for the content of these systems remains at national level.

---

1 Chapter 7 of Opinion 13/31
2 Resolution of the Conference of European Data Protection Authorities

Furthermore, a group of data protection experts (the chairs of all existing joint supervisory authorities, the EDPS and experts from various Member States) also concluded in a report to the conference of European Data Protection Authorities in 2013 that a supervision model in the area of law enforcement such as for Europol "must have the necessary expertise, be able to take decisions and act in a collegiate way, and rely on the necessary means, resources and procedures to be effective." That group also advised that "this mechanism will - to the extent possible - incorporate and build upon the existing forms of cooperation" further "allowing for the flexibility needed to ensure that the specific legal framework is fully respected: for example, by retaining the supervision procedure applicable to Eurojust, or ensuring the specificity of the supervision of Europol and the complaints handling procedure of its Appeals Committee."

The JSB urges that the present provisions for the external data protection supervisor be reconsidered since it considers that they are insufficient, ineffective and do not ensure the necessary consistency.

As in its first opinion, the JSB highlights the importance of establishing an independent and effective joint supervision structure with the equal participation of each national DPA and the EDPS. This joint supervision structure must be independent and have the necessary powers to fulfil its tasks.

To facilitate the establishment of such a structure and especially in the area of administrative support, a link could be made with the supervision structures to be established under the new data protection framework and the revision of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Until then it is strongly suggested that the existing external supervisor - the JSB - be maintained, working in close cooperation with the EDPS, where necessary.

Chapter XIII Transition provisions

The JSB notes that no transitional provisions regulate what will happen on the day of application of the regulation with the existing forms of data processing at Europol. In order to prevent any misunderstanding as to whether or not part of Europol's data processing should stop until the procedure defined in Article 42 is finalised, a transitional period should be introduced.

Conclusion

In its second assessment of the regulation the JSB focused on the consequences of the various provisions in the regulation on Europol's operational activities and on data protection. This second assessment confirms in detail the conclusion of the first JSB opinion that the data protection level presented in the regulation is much weaker than the one provided for by the Europol Council Decision. This assessment also confirms that the regulation will not achieve the intended flexibility for Europol. The flexibility offered by the Europol Council Decision is greater and is combined with effective data protection measures.
The assessment also demonstrates that several tasks Europol is now performing or needs to perform in the near future require its objectives and tasks to be reassessed. The JSB suggests several changes to allow Europol to perform these tasks under tailor-made data protection provisions.

The JSB strongly suggests reconsidering various provisions of the regulation taking into account the arguments and suggestions presented in this opinion. Improvements can be made for Europol and the JSB has presented some suggestions for that purpose.

The JSB is of course always prepared to give further advice and assistance.

Brussels, 9 October 2013

Natasa Pirc Musar
Chair