Opinion of the Joint Supervisory Body of Europol

(Opinion 12/52)

with respect to the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of EURODAC

THE JOINT SUPERVISORY BODY OF EUROPOL

I. Introductory remarks

On 30 May 2012, the Commission presented an amended proposal for a Regulation of the European Parliament and of the Council[1] on the establishment of EURODAC. This proposal introduces access for national law enforcement authorities and Europol to the fingerprint data processed by EURODAC.

In 2009, the Europol Joint Supervisory Body (JSB) expressed as member of the Working Party on Police and Justice[2] its deep concerns about access to EURODAC data for law enforcement authorities. An important element of that concern was - in view of the many other databases and information channels already available - the lack of evidence that such access is actually necessary and proportionate for countering terrorism and other serious crimes.

The Commission's proposal introduces the possibility for Europol to access EURODAC data. As the data protection supervisor of Europol's data processing activities, the JSB considers it its task to give an opinion on this proposal. This opinion focuses on the proposed access for Europol and intends to rectify shortcomings in the current proposal and makes a number of recommendations in this regard.

However, the fact that the JSB has issued this opinion must not be interpreted in such a way that suggests that the JSB therefore considers Europol access to EURODAC is necessary. In fact, the JSB has seen no evidence from the Commission to prove such access is necessary.

Necessity is a fundamental aspect of data protection. The first question the data protection community asks regarding any proposal involving citizen's personal information is always, 'is this necessary?'

- To date, the impact assessments carried out in relation to this proposal have not provided any information demonstrating that it is necessary for Europol to access EURODAC data.
- The citizens whose data are processed in EURODAC belong to a vulnerable group of people whose personal information requires careful handling and - like all other citizens - fair and lawful treatment.

The JSB calls upon the Commission to show that it is necessary for Europol to access EURODAC data.

1 COM(2012)254

2 Press statement July 2009

II. General remarks

Recital 7 of the proposed regulation refers to The Hague and Stockholm Programme calling for improvement of access to existing filing systems and well-targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.

Recital 8 of the proposed regulation states that it is essential in the fight against terrorist offences and other serious criminal offences for law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks.

In using the words "the fullest", the proposed regulation apparently builds further on the availability principle introduced in The Hague Programme. In 2007 the European Data Protection Authorities adopted a common position on the use of the concept of availability in law enforcement[3]. This common position sets out conditions to be complied with for assessing any proposal using availability of personal data as basis and was used to form this opinion, taking into account the specific nature and structure of EURODAC.

Access for Europol to EURODAC data is part of an overall policy to allow law enforcement authorities to have access to these data. Europol's mission to support the EU in preventing and combating all forms of serious international crime and terrorism cannot be seen as separate from the mission of national law enforcement authorities in these crime areas. Article 3 of the Council Decision establishing Europol underlines this, stating that Europol's objective is to support and strengthen action by the competent authorities of the Member States. As a consequence, the assessment of the provisions regarding Europol will have to reflect the general provision of granting access to national law enforcement authorities.

Recital 8 also states that the information contained in EURODAC is **necessary** for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences. However, necessity is not further substantiated, and apparently the proposal assumes that any possibility to identify perpetrators of such crimes via fingerprint comparison can contribute to the fight against crime. Given that the original and continuing purpose of EURODAC is to manage asylum applications, whether or not access to EURODAC data for law enforcement purposes is necessary and proportionate requires a careful assessment and demonstrable evidence, taking into account the vulnerable position of the individuals whose data are processed; a group of individuals who are particularly vulnerable to being singled out and treated differently.

Furthermore, Recital 9 presents conditions that should be met before access to EURODAC is possible. These conditions are:

i) it concerns a terrorist or other serious criminal offence;
ii) there is a substantiated suspicion that the perpetrator has applied for asylum;
iii) there is an overriding public security concern: the criminal act is so reprehensible that it justifies querying databases registering persons with a clean criminal record;
iv) the threshold for authorities to query EURODAC must be significantly higher than the threshold for querying criminal databases.

In addition to the other conditions, conditions iii) and iv), in view of the vulnerable position of the individuals whose data are processed within EURODAC, are apparently intended to underline the justification of access to EURODAC data in specific cases, stating that access should be limited to

[3] Declaration and Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement, Cyprus 11 May 2007, available at http://europoljsb.consilium.europa.eu/about.aspx

those criminal activities which are so reprehensible that querying databases registering persons with a clean criminal record is justified.

These conditions are supplemented with other conditions referred to in Recital 26:

v) systematic comparison should be forbidden;

vi) processing is only on a case-by-case basis. This is further explained as:
a) the request is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence; or
b) to a specific person in respect of whom there are serious grounds for believing that the person will commit or have committed terrorists offences or other serious offences; or
c) the request is connected to a person who is a victim of terrorist offences or other serious criminal offences;

vii) the comparison is necessary for preventing, detecting and investigating terrorist offences and other serious criminal offences;

viii) access is only allowed when a comparison with fingerprint data with the national databases of the Member State and with the Automated Fingerprint Databases of other Member States under the Prüm Decision have returned negative results.

Recital 10, without referring to these conditions, simply concludes that as Europol has a key role with respect to cooperation between Member States' law enforcement authorities, it should therefore also have access to EURODAC.

Recital 12 makes the case for comparing a latent with EURODAC data, for example when it is the only evidence at the crime scene. Whilst the ability to compare a latent against the rolled fingerprint data in EURODAC seems logical, the JSB finds it difficult to understand how authorities could comply with the condition referred to in Recital 9, i.e. that there should be substantiated suspicion that the perpetrator has applied for asylum, simply based on the presence of a latent.

Recitals 24 and 25 introduce designated authorities and verifying authorities to limit and control access to EURODAC. The JSB welcomes that when access is required, this would only be possible by specific and designated authorities and after verification as to whether a request complies with the conditions of the regulation. The JSB also interprets this provision to mean that the verifying authority cannot be the same as the requesting authority, as the alternative interpretation could lead to difficulties in compliance terms.

III. Specific remarks

Articles 5 - 7 and articles 19-21, 28, 33 and 36 regulate the conditions for requests for the purpose of law enforcement. Article 35 contains a prohibition on data transfer to third countries, international bodies or private parties. In this opinion, the JSB assesses these and other articles relevant to the proposed access for Europol to EURODAC data.

Articles 5 and 6 distinguish between designated authorities authorised to access EURODAC and designated verifying authorities tasked to ensure that the conditions set out in the proposed regulation for access are fulfilled. The verifying authority should be a single body responsible for the prevention, detection or investigation of terrorist offences and other serious crime. Articles 5 and 6 could be interpreted to mean that the operating body authorised to request comparisons with EURODAC (Article 5(3)) and the verifying authority could be one and the same. Furthermore, the provisions do not exclude the possibility that the verifying body might be a judicial authority. The JSB recommends that these provisions are made clear.

Article 7 provides for a similar procedure at Europol. Europol should designate a specialised unit as the verifying authority and an operating unit authorised to request EURODAC comparisons.

As it would be impossible to appoint a judicial body as the verifying authority of Europol's requests, it should be ensured that Europol's verifying authority - being part of the same organisation as the operating unit - can ensure independent control on whether the conditions for comparison are actually met. For Europol this will mean that the structure and composition of the verifying authority, as well as its procedures, should guarantee an independent check. The obligation to guarantee independent verification should be introduced in Articles 6 and 7.

Article 19 describes the procedure for comparison and data transmission. It also contains an important element for the verification procedure of the request: the request should be reasoned. This can only be interpreted to mean that it should demonstrate explicitly that it fulfils the conditions allowing a comparison with EURODAC data. A reasoned request is essential for the verification authority, national data protection supervisors and the JSB to fulfil their tasks.

Article 20 sets out the conditions to be complied with for a comparison with EURODAC data. Article 20 applies to national law enforcement authorities and conditions to be met by Europol are described in Article 21. In view of the importance of Article 20 for what should be expected from Europol, the JSB has the following comments on that article.

A comparison between the conditions referred to in various recitals (see chapter II of this opinion nrs. i)-viii) and the conditions of Article 20 shows that not all conditions are presented in Article 20. This is especially the case with the condition referred to in Recital 9 that there should be a substantiated suspicion that the perpetrator has applied for asylum. This omission should be corrected. The other two conditions not mentioned in Article 20:

- there is an overriding public security concern: the criminal act is so reprehensible that it justifies querying databases registering persons with a clean criminal record; and

- the threshold for authorities to query EURODAC must be significantly higher than the threshold for querying criminal databases,

should also be mentioned in Article 20, e.g. as an opening paragraph expressing that access to EURODAC data is only proportionate in these specific situations.

Article 21 sets out the conditions for access to EURODAC for Europol. Paragraph 1 allows comparison of Europol data with EURODAC data when this is within the mandate of Europol and necessary for the performance of its task and for the purposes of a specific analysis or an analysis of a general nature and of a strategic type. No specific conditions - like those for national law enforcement authorities - are foreseen. A striking difference can be found between Article 20(a), which says a comparison should be 'necessary', and Article 21(3)(c), which mentions that a comparison 'will contribute.' In view of Europol's general objective to support and strengthen action by the competent authorities of Member States, it appears that Europol's possibilities to have fingerprints or latents compared with EURODAC fingerprints are much wider than for national authorities. This provision not only opens up the possibility for Europol to systematically compare fingerprints where it is explicitly forbidden for Member States to do so; it also allows the possibility for Member States who are forbidden to check EURODAC (because they are unable to meet the conditions such as checking the Prüm database) to circumvent this safeguard by making their request via Europol.

The JSB repeats that access to EURODAC data should only be possible under specific conditions and in specific cases as described in the various recitals and in Article 20. There is no justification that these conditions should not apply to Europol, especially in view of the vulnerable position of those whose data are processed in the EURODAC system. Article 21 should thus contain the same conditions as set out for law enforcement authorities in Article 20. The condition that national files should be checked first is a condition that should be complied with via the national units in Europol.

In view of Europol's tasks and activities, it may be expected that crime analysis might lead to a situation where linking a fingerprint or latent to a person is necessary for the crime analysis process. One example could be where Europol assists a Member State's investigation in a specific case with crime analysis. In view of the JSB's experience with Europol's data processing activities, such access can only be justified in specific cases and under specific conditions. This comparison can only be done by the Member States involved in a specific investigation or by Europol in compliance with the same conditions set out for the Member States' law enforcement authorities.

Article 21 specifically mentions comparison for the purposes of a specific analysis or an analysis of a general nature and of a strategic type. Although the JSB can imagine conditional access in a specific case, this is not the case where it concerns analysis of a general nature and of a strategic nature. Article 14(4) of the Europol Council Decision (ECD) refers to this type of analysis, which does not focus on a criminal group linked to serious crime but aims to detect trends and patterns and involves cross matching. The necessity to compare fingerprints with EURODAC data for this type of analysis is not evident and does not comply with the Article 20 conditions that should also apply to Europol's access to these data. The reference to this type of analysis should be deleted.

Another aspect of Europol's competence should also be taken into account. According to Article 4(3) of the ECD, Europol's competence shall also cover related criminal offences. What is to be considered as a related criminal offence is further described in that article and could, for example, relate to stealing a vehicle. In view of the wide range of criminal activities which may fall under the concept of related criminal offences, it is difficult to justify access to EURODAC data by simply referring to Europol's mandate.

The JSB repeats that there should be a justification as to why it is deemed proportionate to grant Europol access to EURODAC data. The conditions referred to in Recital 9 clearly indicate that access is not only limited to serious crime but to when, 'the criminal act is so reprehensible that it justifies querying databases registering persons with a clean criminal record.' It is highly questionable as to whether this is the situation with the related crimes referred to in Article 4(3) of the ECD and access to EURODAC regarding these crimes should be excluded.

Article 27(4) obliges Member States and the Agency to inform the Member State of the origin of the data inputted into EURODAC that they have evidence to suggest that data recorded are factually inaccurate. In order to bring Europol's data protection responsibilities for data it processes (Article 29 ECD) in line with Article 27(4), it is suggested to introduce such an obligation for Europol in Article 27(4).

Articles 28 and 36 oblige to keep records (Article 28) of processing operations and the logging and documentation (Article 36).

Article 28 obliges the Agency and Member States to keep records relating to the purpose of access and other data. The purpose of these records is data protection monitoring of the admissibility of data processing as well as to ensure data security. The JSB assumes that this article does not contain an obligation for Europol, since access to EURODAC for Europol can only be created via a National Access Point.

The admissibility of data processing includes the comparison on request of law enforcement authorities of Member States and Europol. As data protection monitoring of the admissibility of these request is performed by national data protection supervisors - and the JSB as data protection supervisor of Europol - it should be ensured that these records will be available for these authorities. A new provision in Article 28 should ensure this.

Article 36 contains similar obligations for Member States and Europol. The obligation to log and document covers, however, all data processing operations resulting from requests for comparison with EURODAC data. Using the word "resulting" might create some misunderstanding about what is meant. "Resulting" can be explained as all data processing activities in the area of law enforcement where the result of comparison is used. Since the obligations in Article 36, like in Article 28, are to be used for checking the admissibility of the requests and monitoring the lawfulness of the data processing, the relation between Article 28 and 36 should be better clarified.

Another aspect that needs attention is the access for Europol via a National Contact Point. The obligations of Article 36 will lead to double logging and documentation of Europol requests: by Europol and by the Member State whose National Contact Point is used by Europol. The obligation of Article 36(2) might then cause problems, especially when the Member State, whose national contact point is used, is not part of the investigation for which the comparison is requested. It could raise security issues (especially in terrorism investigations) and competency issues between data protection supervisors. In this respect it is suggested that the agreement between Europol and the Member State whose National Access Point will be used to communicate Europol's requests to EURODAC (see Article 7), regulates the responsibilities for the obligations of Articles 28 and 36 and the data protection supervision. These agreements will need to be established in close coordination with the data protection supervisors involved. Article 7 should be amended in this sense.

Article 33 regulates the protection of personal data and describes the applicable legislation and some additional limitations for use. Article 33(5) refers to the monitoring by Member States of the lawfulness of processing of personal data under the proposed regulation in the area of law enforcement. Such a reference to the monitoring of Europol is lacking. It is suggested to add to Article 33(2) that the processing of data by Europol shall be supervised by the independent joint supervisory body established by Article 34 of Decision 2009/371/JHA.[4]

Article 35 prohibits onward transfer to third countries, international organisations and private bodies in or outside the European Union, including Interpol. A key aspect to consider is that any access to EURODAC data for law enforcement purposes should never lead to a situation in which the State of origin of the asylum seeker is informed.

Article 14(8) ECD allows - under certain conditions - Europol to invite experts from third countries or international organisations to be associated with the activities of an analysis group. One of these conditions is the existence of an agreement or working arrangement between Europol and the third State or international organisation. These agreements or working arrangements can only be concluded when the level of data protection in those states/organisations is assessed as adequate.
In practice, some of the third States/organisations associated with a specific analysis project are - together with some EU Member States - involved in a specific analysis project focused on an

[4] See also Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218/129, 13.08.2008.

investigation into a specific criminal organisation/activity. When in such an investigation - and in compliance with the conditions of Article 20 and 21- a positive result of a EURODAC comparison is used, a question arises as to whether one of the participants of that investigation - a third State/organisation - may not be informed on the outcome of the comparison. This might in practice create an unmanageable situation. Either the general prohibition remains and Europol and the Member States may not inform a third State or international organisation with whom they jointly investigate a specific crime on the results of a EURODAC comparison, or a specific provision should be developed to allow this under specific conditions. The JSB suggests that this subject is further assessed.

IV. Recommendations

1. Provide hard evidence to prove that is necessary for Europol to access EURODAC data.

2. Europol should not have greater access to EURODAC data than the Member States. Member States without access to EURODAC data should not be allowed to effectively circumvent the law by accessing EURODAC data via Europol.

3. Articles 6 and 7: introduce the obligation to guarantee independent verification. The structure and composition of the verifying authority and its procedures should guarantee an independent check.

4. Article 20: introduce the condition that there should be a substantiated suspicion that the perpetrator has applied for asylum (see Recital 9).

5. Article 20: include - perhaps in an opening paragraph expressing that access to EURODAC data is only proportionate in these specific situations - the following conditions referred to in Recital 9:

- there is an overriding public security concern: the criminal act is so reprehensible that it justifies querying databases registering persons with a clean criminal record; and

- the threshold for authorities to query EURODAC must be significantly higher than the threshold for querying criminal databases,

6. Article 21: include the same conditions set out for law enforcement authorities in Article 20.

7. The necessity to compare fingerprints with EURODAC data for analysis of a general nature and of a strategic type is not evident and will not comply with the Article 20 conditions that should also apply to Europol's access to these data. Delete the reference to this type of analysis.

8. The condition for access to EURODAC that "the criminal act is so reprehensible that it justifies querying databases registering persons with a clean criminal record" does not apply to the related crimes referred to in Article 4(3) ECD and access to EURODAC for these crimes should be excluded.

9. Article 27(4): introduce an obligation for Europol to inform the originator of the data when data appear to be inaccurate, in line with Europol's responsibilities under Article 29 ECD.

10. Amend Article 28 to ensure relevant records would be available for the JSB - the data protection supervisor of Europol - and the national data protection supervisory authorities.

11. Better clarify the relationship between Articles 28 and 36.

12. The agreement between Europol and the Member State whose National Access Point will be used to communicate Europol's requests to EURODAC regulates the responsibilities for the obligations of Articles 28 and 36 and for data protection supervision. These agreements would need to be established in close coordination with the data protection supervisors involved. Article 7 should be amended in this sense.

13. State in Article 33(2) that the processing of data by Europol shall be supervised by the independent joint supervisory body established by Article 34 of Decision 2009/371/JHA.

14. Further assess the question of when Europol and the Member States may not inform a third State or international organisation - with whom they jointly investigate a specific crime - on the results of a EURODAC comparison. Either the general prohibition remains, or a specific provision may need to be developed to allow this under specific conditions.

Done at Brussels
10 October 2012

Isabel Cruz
Chair