Meijers Committee
Standing committee of experts on
international immigration, refugee
and criminal law

Secretariat
p.o. box 201, 3500 AE Utrecht/The Netherlands
phone 0031 30 297 43 28
fax 0031 30 296 00 50
e-mail cie.meijers@forum.nl
http://www.commissie-meijers.nl

[redacted] [redacted]

To (by email) European Parliament
Civil Liberties, Justice and Home Affairs Committee
Rue Wiertz
BE-1047 Bruxelles

Reference CM1216
Regarding Note Meijers Committee on the EURODAC proposal (COM(2012) 254)
Date 10 October 2012

Dear Members of the Civil Liberties, Justice and Home Affairs Committee,

Please find attached a note by the Meijers Committee on the amended proposal for a Regulation on the establishment of Eurodac. The new draft provides for the possibility to request comparison with Eurodac data by Member States law enforcement authorities and Europol. This was also proposed in 2009 but lapsed as a consequence of the Treaty of Lisbon.

The Meijers Committee strongly opposes this access to law enforcement authorities, because it breaches fundamental rights of asylum seekers, including their right to privacy and data protection, the right to asylum and protection against torture and inhuman treatment. Furthermore, the extended use of Eurodac data involves the risk of stigmatisation of a particular group of persons, namely asylum seekers (see section 1 of the accompanying note).
For this reason, the Meijers Committee advises the members of the European Parliament to vote against this proposal.

If the European Parliament decides to accept access for law enforcement authorities and Europol to Eurodac data, the Meijers Committee urges to take into account the comments in the accompanying note (see section 2).

We hope you will find these comments useful. Should any questions arise, the Meijers Committee is prepared to provide you with further information on this subject.

Yours sincerely,

C.A. Groenendijk

Prof. dr. C.A. Groenendijk
Chairman

Note on the proposal for a Regulation on the establishment of Eurodac (COM(2012)254)

1. Access by law enforcement authorities and Europol: a breach of fundamental rights.

The Meijers Committee emphasizes that the proposal by which law enforcement authorities and Europol are permitted access to the information in Eurodac violates fundamental rights of the asylum seekers, including the right to privacy and data protection, the right to asylum and protection against torture and inhuman treatment, and will lead to stigmatisation of this particular group. In earlier comments, the Meijers Committee already expressed its concerns with regard to this access.[1] The Committee is of the opinion that the proposal violates:

- **the right to data protection (Article 8 Charter of Fundamental Rights)**.

The proposed use of Eurodac for law enforcement authorities is originally based on the Regulation (EC) No2725 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention.[2] The proposal to give law enforcement authorities and Europol access to Eurodac will change this database into a criminal law investigation tool which is contrary to the limited purpose of this system, namely the assessment of the state which is responsible for an asylum application under the Dublin Regulation. There would not seem to be a justified exception to the breach of the purpose limitation principle, as the necessity and proportionality of access for law enforcement authorities and Europol have not been demonstrated.
In this context, the Meijers Committee refers to preliminary questions which have been recently submitted by national courts in Germany and the Netherlands to the Court of Justice of the European Union (CJEU) on the implementation of the Regulation(EC) No 444/2009 on standards for security features and biometrics in passports and travel documents issued by Member States.[3] In these questions, the national courts voice their concerns about the proportionality of the central storage of biometric data in passports and travel documents and their use for other purposes and about the relationship of the Regulation with the rights to privacy and protection of personal data safeguarded under Article 7 and 8 of the Charter of Fundamental Rights and Article 8 ECHR. If the CJEU comes to the conclusion that this use is disproportional, access for law enforcement authorities and Europol to Eurodac must most likely also be considered disproportional, considering that these fingerprints are used for another purpose than for which they were stored and that it concerns the systematical storage of fingerprint data of a particularly vulnerable group, asylum seekers.[4]

- **the right to privacy (Article 8 ECHR)**

The underlying proposal gives law enforcement authorities of 31 states and Europol access to a Europe-wide database with the fingerprints of asylum seekers, including minors, who are not suspected of any crime. The presumption that access contributes to the prevention, detection or investigation of the criminal offences is not sufficient to limit the right to privacy and data protection of asylum seekers; a fair balance has to be struck between the competing public interests and the protection of rights of a highly vulnerable group.[5] The Meijers Committee is of the opinion that the European Commission has not given convincing reasons why such a serious infringement is justified. Further, there are insufficient guarantees that data are no longer stored than necessary and that the national authorities of the country of origin of the person who is granted international protection are prevented from accessing the data. Aside from the provision in Article 29, according to which the asylum seeker will be informed on the recipients of his data, he has no means available to challenge the transfer of his fingerprints, initially provided on an obligatory basis for administrative purposes only, to the law enforcement authorities and Europol. The Meijers Committee

[1] See CM0712, CM0714 and CM0910, available on our website www.commissie-meijers.nl.
[2] *OJ* L 50/1, 25.2.2003. Meanwhile the Dublin Convention has been replaced by the Council Regulation 343/2003 (Dublin II) of 18 February. This Regulation is now under consideration (COM(2008) 820).
[3] Dutch Council of State, case 201205423/1/A3, 28 September 2012 and Verwaltungsgericht Gelsenkirchen, C-291/12 *Schwarz v. Stadt Bochum*, 15 May 2012.
[4] In the case of M.S.S. v. Belgium and Greece, it was explicitly underlined that asylum seekers are a highly vulnerable group (application no. 30696/09,21 Januari 2011).
[5] *S. and Marper v. the United Kingdom*, applications nos. 30562/04 and 30566/04, 4 December 2008.

therefore agrees with the opinion of the EDPS that "to intrude upon the privacy of individuals and risk stigmatising them requires strong justification and the Commission has simply not provided sufficient reason why asylum seekers should be singled out for such treatment".[6]

- **the right to asylum and right to protection against torture and inhuman treatment (Article 18 Charter of Fundamental Rights and Article 3 ECHR)**

Extension of the use of data in Eurodac to other authorities not dealing with asylum applications implies the risk that the information will be shared with foreign authorities as well. This risk is enhanced because the information will, through the extended use of Eurodac data, become available to a far wider range of authorities in Member States who have no experience with the specific risks of asylum related information. The mere knowledge that his or her data may be used by law enforcement authorities in the EU and possibly later become accessible to the authorities of the state of origin may already sort detrimental effects on the asylum seeker's right to request asylum or subsidiary protection. In this context the Meijers Committee is also worried about a comment in the recently published note of the Council explaining the need for Europol to be able to request the comparison with Eurodac.[7] According to this note, Europol may use information from third countries, received on the basis of operational agreements according to Article 23 of the Europol Decision (2009/371/JHA), as an indication of 'proving reasonable grounds to consider that a comparison with Eurodac data will lead to the identification of a victim or suspect of serious crime in a specific case'. This use of information by Europol involves the risk that asylum seekers will be labeled as terrorists or suspected criminals by their countries of origin, just to prevent them to obtain asylum in Europe.

- **prohibition of discrimination (Article 14 ECHR)**

The use of fingerprints of asylum seekers for law enforcement purposes and in the fight against terrorism will lead to stigmatisation and discrimination of this group of individuals. This risk of stigmatisation is recognized by the European Court of Human Rights in *S.& Marper v. the UK*.[8] The fact that by this extended use of their information, asylum seekers are de facto considered as suspected persons, may influence the way this group of persons will be treated in society as well.[9] It would have the highly questionable effect of increasing the probability of prosecution of a segment of the population on the mere basis that its members have made use of their fundamental right to seek asylum. A divide will be erected as regards the presumption of innocence between asylum seekers and other parts of the population, which amounts to unequal treatment on the basis of nationality for which no reasonable justification has been advanced.

2. Comments on the new Eurodac proposal

As has been stated above, the Meijers Committee is of the opinion that the comparison and data transmission of fingerprints in Eurodac for law enforcement purposes breaches fundamental rights. The Committee therefore strongly rejects this possibility and advises the LIBE-members to reject the proposal of the European Commission.

[6] Press release Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation on the establishment of EURODAC, 5 September 2012. The recently published note explaining the need for Europol to be able to request the comparison with Eurodac changes nothing to this conclusion, as it is only explained why access contributes to the prevention, detection or investigation of criminal offences but fails to explain why this outweighs the interest of the individuals registered in Eurodac (Note explaining the need for Europol to be able to request the comparison with Eurodac data for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences, Council doc. 14081/12, 21 September 2012.)

[7] Note explaining the need for Europol to be able to request the comparison with Eurodac data for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences, Council doc. 14081/12, 21 September 2012.

[8] *S. and Marper v. the United Kingdom*, applications nos. 30562/04 and 30566/04, 4 December 2008, also judgment of the Bundesverfassungsgericht, 4 April 2006, 1 BvR 518/02 published on 23 May 2006.

[9] In this context, the Meijers Committee also refers to the case Huber v.Germany by the CJEU which has been discussed in an earlier note by the Meijers Committee, see CM0910 accessible through www.commissie-meijers.nl.

If the LIBE Committee decides not to reject the proposal, the Meijers Committee advises to take into account the following comments and suggestions.

1. Designated authorities (Article 5)

According to Article 5(1) Member States shall designate the authorities which are authorised to access Eurodac data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. The Meijers Committee finds that this definition is too wide as it allows Member States to appoint several different national authorities having access to the data in Eurodac. In this context, the Meijers Committee recalls the standard case law of the European Court on Human Rights stating that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants rights' under Article 8.[10] The possibility in Article 5 (1) for Member States to designate a large number of "designated authorities" authorised to have access to the Eurodac data will hamper the effective control on the use and further storage of the fingerprints of asylum seekers. The obligation of Member States to notify the Commission of the lists of the designated authorities is insufficient in this respect (Article 43 of the proposal).

The wide definition of "designated authorities" leads to a further interference of Article 8 ECHR. The Meijers Committee strongly advises to limit the possibility for Member States to designate law enforcement authorities who may access Eurodac, by developing limitative lists in the Regulation itself, or in an annex, of the national authorities authorized to have access to Eurodac data.

2. Data storage and advance data erasure of applicants for international protection (Article 12, Article 13)

Data of applicants for international protection shall be stored for ten years from the date on which the fingerprints were taken. When a person acquires citizenship before the ten-year period has lapsed, his data shall be erased from the Central System "as soon as the Member State of origin becomes aware that the person has acquired such citizenship". The Meijers Committee finds that this provision gives too much discretion to the Member State. It is necessary that Member States keep track of changes in the situation of the persons registered in Eurodac as there is an implementation deficit in the advance deletion of data. In the Eurodac Activity report the EDPS mentions "that inspections were carried out and results made clear that some Member States still lacked appropriate procedures for dealing with advance deletion".[11] This indicates that data remain to be stored in Eurodac while they should have been erased. The Meijers Committee is particularly concerned about this in the context of access by law enforcement authorities and Europol: if data are stored longer than necessary it gives them even wider access to data of persons who are not suspected of any crime. With regard to this problematic issue and in line with the recommendations of the European Data Protection Supervisor, the Meijers Committee proposes the following:

- **efficient procedures for automatic advance deletion of data by Member States should be established;**
- **if law enforcement agencies and Europol should gain access to Eurodac data, the Regulation should include strict and short time limits for the storage of the data on asylum seekers.**

3. Comparison of fingerprint data (Article 17)

From an inspection report by the EDPS of the EU's Eurodac Central Unit it appears that comparisons of fingerprint data of a third country national or a stateless person found illegally staying within its territory with the fingerprints registered in Eurodac are not deleted once these comparisons have been transmitted to

[10] ECHR Leander v. Sweden appl.no. 9248/81, 26 March 1987 and ECHR Weber and Saravia v. Germany, appl.no.54934/00, 28 October 1994.
[11] European Data Protection Supervisor "Coordinated Supervision of Eurodac Activity Report 2010-2011", p. 6, 4 July 2012.

relevant Member States, contrary to the obligation under Article 11(5) of the current Eurodac regulation.[12] This is a clear violation of the obligation to ensure that data are not stored longer than is necessary for the purposes for which data were collected. The Meijers Committee therefore questions the decision to delete the obligation for the Central Unit to erase the results of the comparison in the new Article 17. Especially now that access for law enforcement authorities and Europol is allowed and data become available for a large group of authorities it should be guaranteed that the Central Unit will delete the results of the comparison immediately after it has been transmitted. The Meijers Committee urges that comparisons as regulated in Article 17 must be deleted immediately after these data have been transmitted to the Member States. Therefore, this obligation that is provided in Article 11(5) of the current Eurodac Regulation (2725/2000/EC) should be maintained:

> **Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:**
> **(a) erase the fingerprint data and other data transmitted to it under paragraph 1; and**
> **(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.**

4. Marking of data (Article 18)

Article 12 of the current Eurodac Regulation (2725/2000/EC) regulates that data relating to an asylum applicant are blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Hits concerning these persons are not transmitted and the Central Unit should send a negative result to the Member State. Although the data remain in the Central Database, these data are not accessible by the Member States as long as the person is recognized as a refugee. If the refugee lost his status as a refugee, his data would be unblocked. Under the new proposal, data of persons who are granted international protection are marked: "this mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5)". This means that data are no longer blocked, but can be transmitted to the Member States, even if the applicant has been granted international protection. The Committee wonders whether "for the purposes of transmission under Article 9(5) (application for international protection)" means that data shall not be transmitted when these data are requested by law enforcement authorities and Europol. The Meijers Committee suggests the following amendment, in the line of Article 12 of the current Eurodac Regulation:

> **Data relating to an applicant for asylum which have been recorded pursuant to Article 11 shall be blocked in the central database if that person is recognised and granted international protection in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member States of origin.**
> **Hits concerning persons who have been recognised and granted international protection in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.**
>
> **Furthermore, the question whether "for the purpose of transmission under Article 9(5)" in the new Article 18(1) means that data shall not be transmitted when these data are requested by law enforcement authorities and Europol should be clarified.**

5. Conditions for access to EURODAC data by designated authorities and Europol (Article 19 to Article 22).

The Meijers Committee emphasizes the vulnerable position of asylum seekers and the obligation of Member States to protect the right to asylum under Article 18 of the EU Charter on Fundamental Rights and their right of non-refoulement under the Geneva Convention and Article 3 ECHR. It is therefore even more important that the conditions for access to Eurodac by designated authorities and Europol are strictly and clearly defined. For this reason, the Meijers Committee is worried about the possibility regulated in Article 19(3) that "in exceptional cases of urgency, the verifying authority may transmit the fingerprint data immediately to the requesting authority, and only verify ex-post whether all the conditions of Article 20 or Article 21 are fulfilled.

[12] EDPS Eurodac Central Unit Inspection report June 2012, Council doc. 11660/12.

"Exceptional cases of urgency" is too vague and should be clarified. The Meijers Committee supports the suggestion by the EDPS to add the criterion 'of the need to prevent an imminent danger associated with serious criminal or terrorist offences'.

The Meijers Committee has noticed that in Article 20 (1) (c) the word "substantially" is no longer mentioned, which makes the condition for access broader and less clear than in the Eurodac proposal of 2009. In the Council Decision concerning access for consultation of the Visa Information Systems (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 access is only possible when "there are reasonable grounds to consider that consultation of VIS data will *substantially* contribute to the prevention, detection or investigation of any of the criminal offences in question". Eurodac contains information of vulnerable persons and conditions to access this data should be at least as strict as access to VIS. The Meijers Committee suggests to amend Article 20 (1)(c) as follows:

There are reasonable grounds to consider that such comparisons with Eurodac data will *substantially* contribute to the prevention, detection or investigation of any of the criminal offences in question.

The Meijers Committee is concerned that the conditions for access to Eurodac data by Europol are broader than the conditions for access by designated authorities. The Committee welcomes the suggestions by the Presidency to align the conditions for access by Europol with the conditions for access by designated law enforcement agencies. This was also suggested by the EDPS in its opinion.[13]

6. Role national supervisory authority (Article 29 to Article 32)

The Meijers Committee supports the explicit role given to the European Data Protection Supervisor and the National Supervisory Authorities in the supervision of data processing activities concerning Eurodac. The access for law enforcement authorities to the sensitive data of asylum seekers in Eurodac must be strictly supervised. However, the Committee is worried that the supervision of access for law enforcement authorities and Europol means a further extending of their tasks. With the adoption of various data processing instruments in the last decennium there has been an increasing workload, which has not been accompanied by an increase of financial means and capacity. The Committee therefore recommends that:

It should be guaranteed that both the national and European supervisory authorities are provided with sufficient financial and personal resources to be able to supervise the use and access to Eurodac data adequately.

7. Exchange of data with third countries (Article 35)

In Article 35 it is stated that personal data obtained by a Member State or Europol from the Eurodac database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This provision does not prevent that Eurodac data, when stored in the national data bases of EU or Dublin States will be transferred to third states outside the framework of the Dublin Regulation. The Meijers Committee therefore proposes to add to Article 35 (in italics):

Personal data obtained by a Member State or Europol pursuant to this Regulation from the Eurodac central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies. *Personal data obtained by a Member State or Europol and processed further in national databases, shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union.*

[13] Presidency compromise suggestions, 13884/12, 20 September 2012 and opinion of the EDPS, paragraph 59, 5 September 2012.