Permanente commissie
van deskundigen in
internationaal vreemdelingen-,
vluchtelingen- en strafrecht

Secretariaat
postbus 201, 3500 AE Utrecht/Nederland
telefoon 31 (30) 297 42 14/43 28
telefax 31 (30) 296 00 50
e-mail cie.meijers@forum.nl
http://www.commissie-meijers.nl

[redacted] [redacted]

To Mr. Jacques VERRAES
Directorate D: Internal security and criminal justice
European Commission
Directorate General Justice, Freedom and Security
B-1049 Brussels BELGIUM

Reference CM0714

Regarding Proposal to give law enforcement authorities access to Eurodac

Date 6 November 2007

Dear Mr. Verraes,

The Standing Committee is most grateful for the opportunity the services of the European Commission provided during the meeting on 8 October 2007 to express our views on the intended proposal to give law enforcement authorities access to Eurodac. We appreciate the openness of the Commission and the insight you gave in the intended legislative measures developed so far.

However, we still have serious concerns as to the legality and the usefulness of this possible proposal. There are five core arguments why the intended proposal in our view would be unlawful: firstly, access to Eurodac data for law enforcement authorities would be irreconcilable with the present purpose limitation of the Eurodac regulation, secondly, there is no legal basis in EC law for extending the use of Eurodac with security purposes. Thirdly, such an extension is incompatible with basic principles of European law, international standards, and constitutional law of the Member States, the observance of which the Court of Justice ensures[1]. Fourthly, data protection authorities lack sufficient means to protect the rights of asylum seekers and fifthly, the proposal will affect the integrity of Eurodac. We will explain below, why in our view the intended measures are vulnerable for annulment by the Court of Justice.

1. No legal basis in EC Treaty for extending Eurodac purpose with security goals

The present purpose of the Eurodac regulation gives no room for granting access to its data to law enforcement authorities. During the October 8 meeting it was contended that a modification of the purpose of Eurodac would suffice to assure the lawfulness of the intended proposal. However, there is no legal basis in the EC Treaty for the intended extension of the purpose of Eurodac with security (criminal law and intelligence) purposes. According to its preamble, the legal basis for the Eurodac regulation is Article 63(1)a EC Treaty. Article 63(1)a does not provide any reference whatsoever as to police and intelligence goals. Further, it is expressly laid down in this Treaty provision that measures based on Article 63(1) must be "in accordance with the Geneva Convention of 28 July 1951 and the Protocol of 31 January 1967 relating to the status of refugees and other relevant treaties". Even when interpreting Article 63(1)a EC Treaty extensively, the Standing Committee is unable to see how security goals could be deemed to be covered by this provision. Rather, the explicit referral to the Refugee Convention and other relevant treaties stand in the way to such an interpretation.

2. Incompatibility with international law, principles of Community law and constitutional law of Member States

In our opinion, the planned legal measures disregard that any change of the Eurodac Regulation or any other measure based on the EC Treaty or the EU Treaty has to be in conformity with the principles of Community law and with the

[1] See for instance Parliament v. Council, Case 540/03, CoJ 27 June 2006, para 35.

relevant international treaties binding all Member States. The intended proposal raises serious questions as to its compatibility with: (a) the 1951 Refugee Convention, (b) the European Convention on Human Rights, (c) the EU Charter of Fundamental rights and (d) the constitutional principles of Member States.

Ad (a) 1951 Refugee Convention
Central in our view is the unacceptable risk caused by using the Eurodac data outside the strictly limited circle foreseen in the present Eurodac Regulation. However tight the conditions for access of law enforcement authorities to Eurodac data may be, once the information is outside the "Eurodac circle", it will be impossible to control what happens with these data afterwards. At the hearing we understood that the Eurodac data are only relevant for investigation or prosecution purposes if the police on the basis of the Eurodac will get access to further information from the file of asylum applicant from the immigation authorities. As we stated at the hearing and supported by – amongst others – UNHCR, there is a real danger that asylum information may reach countries of origin and thus endanger asylum seekers. In this respect it would be unrealistic to rely on data protection authorities who are not equipped for this task and who are lacking the personal and financial resources (see point 4 below).
The Geneva Convention has been ratified by all Member States. Under Article 35 Refugee Convention it is the task of the UNHCR to supervise the application of the provisions of the Refugee Convention. Hence, these concerns that were also raised by UNHCR during October 8 meeting, should be taken most seriously.
Further, there is a serious risk that refugees will refrain from filing an application for protection in an EU Member State once they become aware that information provided in respect with their asylum claim might be shared with police, criminal law and intelligence officers in all Member States and via those officers or through Europol with authorities of their country of origin or other third countries. This sharing of information may also increase the risk of bad or even inhuman treatment of relatives or friends of the refugee living in the country of origin by the authorities of that country. Finally, it may also increase the chances of bad or inhuman treatment of the applicant by those authorities in case the applicant for asylum after rejection of his request for asylum has to return to that country.

Ad (b) European Convention on Human Rights
According to Article 6(2) of the EU Treaty, the Union respects the fundamental rights as guaranteed in the ECHR. The ECHR is undoubtedly one of the "other relevant treaties" referred to in Article 63(1) of the EC Treaty. According to Article 3 ECHR, protection against torture or inhuman treatment is absolute regardless of any consideration of public policy or security[2]. The protection of Article 3 is relevant considering the serious risk that not only the asylum seeker after return, but also his family members, friends or fellow-party members in the country of origin may be subject to inhuman treatment if the information from the asylum file will leak to the countries of origin of asylum seekers, because that information will, through the extended use of Eurodac data, becomes available to a wider range of authorities in Member States who have no experience with the specific risks of asylum related information.

Ad (c) EU Charter of Fundamental rights
The Reform Treaty will confirm the binding character of the EU Charter of Fundamental Rights. The following rights granted by this EU Charter are relevant in this respect.

1) With regard to the duty of Member States to protect the safety of asylum seekers, preventing that their personal data becomes available to authorities of the country of origin:

Article 6 - Right to liberty and security
Everyone has the right to liberty and security of person.

2) With regard to the collection and extended use of fingerprints and the inherent violation of the privacy rights of asylum seekers:

Article 7- Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.

[2] See for instance the Chahal judgment, ECtHR 25 October 1996, app. 70/1995/576/662, para. 106

3) With regard to the duty of Member States to safeguard the integrity of Eurodac, to respect the principle of purpose limitation, to prevent unauthorised access to Eurodac data, and to guarantee effective and independent supervision by data protection authorities:

Article 8 - Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

One of the most important principles of data protection law is the *purpose limitation principle* according to which personal data can be processed as long as the processing meets *specified, explicit, and legitimate* purposes[3]. As this principle is laid down in instruments binding on all Member States, it must be considered a principle of Community Law.

4) With regard to the duty of Member States to make sure that persons who are in need of refugee protection have the right to apply for asylum and are not refrained from doing this because of knowing that their data will be used by law enforcement authorities or and security agencies:

Article 18 - Right to asylum
The right to asylum shall be guaranteed with due respect for the rules of the Geneva Convention of 28 July 1951 and the Protocol of 31 January 1967 relating to the status of refugees and in accordance with the Treaty establishing the European Community.

5) With regard to the duty of Member States to protect asylum seekers against refoulement:

Article 19 - Protection in the event of removal, expulsion or extradition
1. Collective expulsions are prohibited.
2. No one may be removed, expelled or extradited to a State where there is a serious risk that he or she would be subjected to the death penalty, torture or other inhuman or degrading treatment or punishment.

Ad (d) constitutional principles of Member States
Using Eurodac data for law enforcement goals is unlawful, because it would amount to a breach of the fundamental right to privacy guaranteed in the constitutional law of several Member States. In that respect, the view of the Standing Committee is supported by the judgment of the German Constitutional Court, on the practice of '*Rasterfahndung'* or data profiling by the German police in their fight against terrorism.[4] In this judgment of 2006, concerning the complaint of a Moroccan student, the Court held the practice of the German police authorities of data profiling ('*Rasterfahndung'*) unlawful, because it would include a disproportional breach of the constitutional right to privacy. For this conclusion, the German Court explicitly referred to the extended scope of the collection of information, the use of many different data bases, the increased risk for the person concerned to become a target of criminal investigation, and the possibility of stigmatisation of a group of persons in public life.
According to the Constitutional Court, such a measure could only be justified on the basis of a concrete danger of a terrorist attack which would cause great harm and which risk could be based on concrete facts. The Court considered

[3] This principle provides the criteria to decide about the legitimacy of a processing and the use and quality of the personal data processed. The principle of purpose limitation not only requires the availability of a specific goal for data processing, but also implies the legitimacy of this goal. This principle of a legitimate purpose is included in Article 5 of the Data Protection Convention, but also in Article 7 of the EC Directive 95/46 which goes further. According to Article 7 of the EC Directive, data processing is only legitimate if:
- the data subject has given his consent;
- the data processing is necessary for a contract to which the data subject is a party;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- it is necessary in order to protect the vital interests of the data subject; or
- for the performance of a task in the public interest or in the exercise of an official authority vested in the controller or in a third party to which the data are disclosed and, finally;

when processing is necessary for the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests are overridden by the fundamental rights and interests of the data subject.
[4] Judgment of the Bundesverfassungsgericht, 4 April 2006, 1 BvR 518/02 published on 23. May 2006.

that the general situation of threat which exists since 11 September 2001 or a tense situation based on foreign policy matters are no sufficient reasons to justify the practice of data profiling.

3. SIS-II and VIS are no precedents

During the October 8 hearing it was repeatedly stated that the use of SIS-II and VIS for security purposes had been accepted by the Council and the Parliament and thus provided good precedents for extension of the purpose of Eurodac.
The Standing Committee maintains that there are several essential differences between Eurodac and the two other EU systems with data on immigrants. Firstly, SIS-II and VIS have a different legal basis and accordingly another purpose[5]. The much stricter purpose of Eurodac and its legal basis in Article 63(1)(a) EC Treaty do not allow extension of the use of its data neither by way of a regulation under the first pillar, nor by way of a framework decision under the third pillar.
Secondly, the large majority of persons whose data are registered in Eurodac are asylum seekers. In contrast, asylum seekers or persons in need of protection will be only a tiny minority of the registered in VIS or SIS-II. Hence, the risk that the negative side-effects of the extension of the use of Eurodac will actually occur, is far greater than with the use of data in VIS or SIS-II for security purposes.
Thirdly, in SIS-II only data are registered concerning persons selected by authorities of Member States in relation with a criminal investigation or a conviction or on the basis of a concrete immigration law concern. In Eurodac data on all asylum seekers are stored, without any selection. Moreover, an asylum seeker is not free. He is obliged to give his fingerprints. He has no alternative if he wants to apply for international protection. The position of an asylum seeker in that respect is clearly different from any third-country national visitor who may decide to apply for a visa or not, once he becomes aware of the possible side-effects of his registration in VIS[6]

4. Limited role of data protection authorities

The Standing Committee wishes to emphasize that it is unrealistic to rely on data protection authorities in order to supervise the rights of asylum seekers whose data are being stored into Eurodac or the use of those data in relation with further information from the asylum file of an individual asylum seeker. Currently, national and European data protection authorities are not equipped for this task, because of lack of personal and financial resources. In 2003 in its first evaluation report of the EC Directive 95/46, the Commission itself expressed its concerns about the lack of independence of data protection authorities in the Member States, due to a lack of sufficient resources.[7] In this report, the Commission pointed out to the presence of three inter-related phenomena:

- *An under-resourced enforcement effort and supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority;*
- *Very patchy compliance by data controllers, no doubt reluctant to undertake changes in their existing practices to comply with what may seem complex and burdensome rules, when the risks of getting caught seem low;*
- *An apparently low level of knowledge of their rights among data subjects, which may be at the root of the fact that the Commission received relatively a small number of individual complaints.*

The Commission emphasized in its report that independence in the taking of decisions is a *sine qua non* for the correct functioning of the system of supervision by national data protection authorities and that resource difficulties may affect independence. Currently, national data protection authorities are still lacking sufficient resources and therefore the conclusions of the Commission are still valid.
By way of example, we refer to the alarming letter of the chairman of the Dutch Data Protection Authority of August 2007, in which he states that due to a lack of financial resources, his organisation is forced to reduce its supervisory tasks.[8] According to the chairman, the Dutch Data Protection Authority is no longer able to deal with every individual complaint. He explicitly referred to the fact that his organisation was unable to perform its controlling task with regard to important developments at the international level and the use of biometrics.
If the rights of individuals are infringed by the use of large-scale databases such as Eurodac and data protection authorities are not able to apply intensive supervision and to offer effective remedies, this may also result in a violation of Article 8 ECHR (and Article 7 and 8 of the EU Charter). We refer in this regard to the judgment of the European Court of

[5] The SIS-II regulation has its legal basis in Articles 62(2)(a), 63(3)(b) and 66 EC Treaty, the adopted text of the VIS regulation has its legal basis in Article 62(2)(b)(ii) and 66 EC Treaty.
[6] This does not mean however that the Standing Committee fully agrees with the extended use of VIS, see our earlier comments on this subject www.commissie-meijers.nl
[7] COM (2003) 265, 15.5.2003, p.12-13.
[8] Memorandum *Handhaven vereist middelen*, 8 August 2007.

Human Rights (ECtHR) in the case of *Segerstedt-Wiberg v. Sweden.* [9] In this judgment, the Court dealt with the lack of powers of the Swedish Data Protection Authority (Data Inspection Board), with which individuals could lodge a complaint. The ECtHR concluded that it had not been shown that the available procedure carried out by the Data Inspection Board offered an effective remedy in practice with regard to an application for deletion of the data (§ 120). According to the ECtHR, no information had been furnished "to shed light on the effectiveness of the Data Inspection Board in practice". On the contrary, during this procedure (which dealt with the storage of personal information by the Swedish Security Police), the applicants alleged that during its 30-year existence, the Data Inspection Board had never performed a substantial review of the files held by the Security Police.

5. Risks for the integrity of Eurodac and the Dublin system

Once it becomes known that the data in Eurodac are used for other purposes, it is to be expected that refugees and other persons in need of international protection will refrain from filing a formal application for asylum in order to avoid the risks mentioned above. Besides, they may be inclined to mutilate their fingers in order to make their fingerprints unusable. Both effects will endanger the original purpose of Eurodac: to assist the effective implementation of the Dublin system.

Access by law enforcement authorities to Eurodac data also implies the risk that data on asylum seekers in this database, which should have been deleted according to the Articles 7, 10 and 12 of the Eurodac Regulation, will continue to be stored and used by national authorities, without further control with regard to the unlawful storage of these data. In the current practice of Eurodac it appears to be difficult to delete the data in accordance with the rules of the Eurodac Regulation. For example, the Dutch Minister of Justice, answering parliamentary questions, had to admit that in 2007 there was still no mechanism available to assure that asylum seekers who obtained the status of refugee, were issued a residence permit or were naturalised would be automatically deleted from Eurodac, as provided in the Eurodac Regulation.[10] The result of this practice and the proposed extension of the use of Eurodac would be that data on recognised refugees or EU citizens remain registered in Eurodac and could be used for police and intelligence purposes.

Safeguarding the integrity and reliability of data not only protects individual refugees and asylum seekers, it also ensures the accuracy of the systems being used and thus the mutual trust between national authorities.[11]

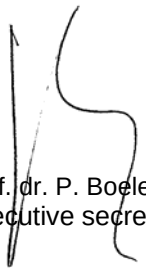
Conclusion

We most strongly advise against the intended legislation to amend the Eurodac regulation because it would be unlawful and thus would risk to be annulled by the Court of Justice. As pointed out extensively above, there are five core arguments why the intended legislative measures would be unlawful: firstly because access to Eurodac data for law enforcement authorities would be irreconcilable with the present purpose limitation of the Eurodac regulation, secondly because there is no legal basis in the EC Treaty for extending the purpose with security purposes, thirdly, because the purpose extension would be incompatible with obligations under international treaties ratified by all Member States and with relevant principles of Community Law, the observance of which the Court of Justice ensures. Fourthly, data protection authorities lack sufficient means to protect the rights of asylum seekers and fifthly, the proposal will affect the integrity of Eurodac.

We send a copy of this letter to other participants at the meeting of 8 October 2007, among others UNHCR Brussels, ECRE, Amnesty International, the LIBE Commission, the European Data Protection Supervisor and to the Dutch Refugee Council, the latter organisation being one of the five organisations that established our Committee.

Yours sincerely,

Prof. dr. C.A. Groenendijk
Chairman



Prof. dr. P. Boeles
Executive secretary

[9] Segerstedt-Wiberg v. Sweden, 6 June 2006, no. 62332/00, §§ 118-122.
[10] Handelingen Tweede Kamer 2006-2007, Aanhangsel 679, question 317 (official publication of Dutch Parliament).
[11] See also the European Data Protection supervisor in its opinion of 19 December 2005 on the draft Framework Decision for Data Protection in the third pillar, *OJ* C 47/27, 25.2.2006, consideration 5.