

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

*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>

■ ■  
**To**

European Parliament  
Civil Liberties, Justice and Home Affairs Committee  
Rue Wiertz  
BE-1047 BRUXELLES

**Reference  
Regarding**

CM0910  
The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), 10.09.09.

**Date**

30 December 2009

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

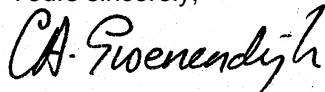
Please find attached the note of the Meijers Committee (Standing Committee of experts on international immigration, refugees and criminal law) on the amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), 10 September 2009.

The Meijers Committee, sharing the serious concerns of the European Data Protection Supervisor and the national data protection authorities, strongly advises the members of the European Parliament to vote against this legislative proposal of the European Commission on the following grounds:

- The proposal runs counter to fundamental data protection principles such as proportionality of data processing and respect for purpose limitation.
- The proposal 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.
- The proposal will lead to stigmatisation of this particular group of asylum seekers, in violation of the principle of non discrimination.
- When adopted, there is a serious risk that these instruments (the proposed Decision and Regulation) will invoke preliminary questions by national courts and subsequently will be held unlawful by the European Court of Justice, considering recent jurisprudence of both the European Court of Justice and the European Court for Human Rights.

Should any questions arise, the Standing Committee is prepared to provide you with further information on this subject.

Yours sincerely,



Prof. dr. C.A. Groenendijk  
Chairman

---

• **Meijers Committee**

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

• **Comité Meijers**

Comité permanent d'experts en droit  
international de l'immigration,  
des réfugiés et du droit pénal

• **Meijers-Ausschuss**

Ständiger Ausschuss von  
Experten im internationalen  
Ausländer-, Flüchtlings- und Strafrecht

**Note by the Meijers Committee on the amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), 10 September 2009****Introduction**

The Meijers Committee took note of the Commission's proposal for the amendment of the Eurodac Regulation and the Decision by which national law enforcement authorities and Europol may, under certain circumstances, gain access to data on asylum seekers stored in Eurodac. In earlier letters, the Meijers Committee already expressed its deep concerns with regard to this proposal. These concerns have been repeated during a meeting with other NGO's organised by the European Commission on 8 October 2007. The underlying proposal and the explanatory memorandum to this proposal establish that the Commission did not sufficiently take into account the concerns put forward by the different NGO's and the data protection authorities. For example, in the explanatory memorandum to the draft Decision, the Commission, giving a "summary of responses and how they have been taken into account", only mentions that Member States were very favourable to having the possibility to compare fingerprints with Eurodac for law enforcement purposes, while civil liberties and asylum NGOs were not. The general conclusion of the Commission that this proposal presents a balance on the positions of the various interested groups, by containing several guarantees and limits, cannot be sustained. The Meijers Committee shares the concerns of the European Data Protection Supervisor in his opinion of 7 October 2009, expressing his serious doubts on the legitimacy of the proposal and the fact that the necessity of the proposal has not been proven. The Meijers Committee also shares the deep concerns of the national data protection authorities, represented in the Working Party on Police and Justice (WPPJ), stating that the proposal runs counter to fundamental data protection principles such as proportionality of data processing and respect for purpose limitation (September 2009). The Meijers Committee advises the members of the European Parliament to vote against this legislative proposal.

The Meijers Committee emphasizes that the intended measure in this proposal by which law enforcement authorities and Europol gain 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. Considering recent jurisprudence of both the European Court of Justice and the European Court for Human Rights, it is clear that it is only a matter of time before these instruments (the proposed Decision and Regulation) when adopted, will invoke preliminary questions by national courts and subsequently will be held unlawful by the European Court of Justice.

In the following sections, the Meijers Committee will shortly describe the content of the current proposal and set out why the proposed access to law enforcement authorities is in breach of fundamental rights: Article 8, 3 and 14 ECHR, Article 8 EU Charter, EC Directive 95/46, and asylum law.

**1 Content of the proposal**

The current proposal finds its origin in the general policy of EU Member States developed since 2001, to improve the exchange of data in order to strengthen security, also emphasized in the The Hague program. In its meeting of 12-13 June 2007, the JHA Council invited the Commission to present a proposal by which national law enforcement authorities could gain under certain circumstances access to Eurodac. The current proposal amends an earlier proposal of the European Commission amending Regulation 2725/2000 of December 2008 (COM (2008) 825), designed to ensure a more efficient use of Eurodac and addressing some data protection concerns. For example, the December proposal envisages a better management of deletions of data from the central database by ensuring that the Central System informs Member States of the need to delete data. Based on the amended Regulation, data on every applicant for asylum (in this proposal for international protection) of at least 14 years of age remain to be stored into Eurodac for ten years, however data on persons apprehended in connection with the irregular crossing of the external borders will be stored for one year instead of two years. Furthermore, this proposal provides that the list of authorities having access to Eurodac will be published in the Official Journal of the European Union.

In the proposed text of the Regulation and Decision of September 2009, the power of law enforcement authorities and Europol to gain under certain circumstances access to Eurodac data is provided in Article 3 of the proposed Regulation. This provision contains three material limitations on the intended access by law enforcement authorities and Europol to the data registered into Eurodac. Firstly, the aforementioned authorities may ask only for comparison of fingerprint data in Eurodac if a comparison of data stored in national fingerprint databases on the basis of the Prüm Decision (Decision 2008/615) returned negative results. Secondly, the comparison must be necessary “in a specific case.” Thirdly, there must be reasonable grounds to consider that the consultation of data stored into Eurodac will substantially contribute to the prevention, detection, or investigation of terrorist offences and of other serious criminal offences. The comparisons will be carried out through “verifying authorities” established according to Article 4 of the proposed Decision. In “an exceptional case of urgency” this verifying authority may receive written or reasoned logged electronic requests and verify only ex-post whether all the conditions for access were fulfilled, including whether an exceptional case of urgency existed. This ex-post verification must take place “without undue delay after the processing of the request”.

According to Article 3 (3) of the Regulation neither the hit nor the data obtained from Eurodac shall be transferred or made available to a third country, international organisation or a private entity established in or outside the EU. Article 12 of the proposed Decision includes an exception of this principle, stating that Member States retain the right to transfer data to third countries (Norway, Iceland, and Switzerland) to which the Dublin Regulation applies, provided that the condition of Article 13 of Framework Decision 2008/977 on data protection in the framework of judicial and police cooperation are fulfilled. It should be noted that this latter provision, describing the conditions in which data can be transferred to authorities in third states or Europol, leaves the Member States a wide margin of discretion to decide whether they want to transfer data to these countries or whether these countries provides “adequate safeguards”. Considering the level of data protection in these third countries, it should be taken into account that these countries are not bound by the Framework Decision 2008/977 or the Directive 95/46 on the protection of personal data.

## **2 Right to privacy – Article 8 ECHR**

### *Interference with the right to privacy*

It is significant that in the accompanying impact assessment, the European Commission only considers the impact of this proposal with regard to the right to data protection, as protected in Article 8 of the EU Charter on Fundamental Rights, but does not take into account the right to privacy, protected in Article 8 ECHR. The Meijers Committee emphasizes that this is a significant omission, especially considering the case law of the ECtHR in which it was made clear that large-scale databases including fingerprints of individuals fall within the scope of this fundamental right. In *S. & Marper v. the United Kingdom*, the ECtHR dealt with the long-term, systematic storage of fingerprints and DNA samples of individuals, including minors, who were suspected of having committed criminal offences, but who were not convicted.<sup>1</sup> In para. 81 of this judgment, the ECtHR stated that fingerprints records constitute personal data containing certain external identification features comparable to photographs or voice samples. Even if fingerprints constitute neutral, objective and irrefutable material and, unlike photographs, were unintelligible to the untutored eye and without a comparator fingerprint, the ECtHR found that fingerprints contain “unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances”. Thus, according to the ECtHR, they “are capable of affecting his or her private life and retention of this information without the consent of the individual can not be regarded as neutral or insignificant”. (para. 84).

In this judgment, the ECtHR had to assess the legitimacy of a “nationwide database with the aim of permanently kept and regularly processed by automated means for criminal-identification purposes”. The Court found that the applicable UK law violated Article 8 ECHR, particular on the grounds that these data were stored for indefinite periods and also concerned unconvicted persons as disproportional. Furthermore, the ECtHR, referring explicitly to fingerprints as belonging to special categories of more sensitive data (para. 103), warned against the risk of the stigmatising effect (see further below). The Meijers Committee recalls that the underlying proposal on Eurodac concerns a *European wide database* with the fingerprints asylum seekers, irrespective if these persons were ever

---

<sup>1</sup> *S. and Marper v. United Kingdom*, 4 December 2008, appl.no. 30562/04 and 30566/04.

involved in any criminal procedure, and whose data will be accessible by the law enforcement authorities of 30 states and Europol. Furthermore, referring to the ECtHR's conclusions on the indefinite retention of fingerprints and DNA in the Marper case, it should be noted that even if the Eurodac Regulation and the new proposal provide in the deletion from the Central System of data after ten years, they do not provide any safeguards with regard to the national practice. These texts do not prevent that fingerprints collected and stored on the basis of the Eurodac Regulation will be retained for a longer period by the national authorities in their national databases.

*Necessary in a democratic society*

To meet the requirements of Article 8 ECHR, the proposed access to law enforcement authorities and Europol should be necessary in a democratic society in order to reach a legitimate purpose mentioned in Article 8 (2) ECHR, and must be in accordance with the law. In the impact assessment to the proposal, the Commission only considers these requirements when dealing with the requirements of Article 8 of the EU Charter on the right in data protection. Although as we will see below, the ECJ confirmed that the EC Directive 95/46 on the protection of personal data must be interpreted in accordance with the right to private life in Article 8 ECHR, it should be underlined that the right to data protection is not synonymous with the right to privacy, and considering the jurisprudence of the ECtHR when dealing with Article 8 ECHR, stricter criteria may be applied when the right to private life is at stake. At this point, it has to be taken into account that the current proposal concerns the information of asylum seekers, whose position, as will be dealt with further in section 3, is highly vulnerable. For this reason, it is clear that with regard to the balance to be made between the interests of the state and the interests of the asylum seeker on the basis of Article 8 ECHR, much stricter standards must be applied. As we will set out in section 2, it also questionable whether the current proposal meets the standards of the general principles of data protection law.

Considering the protection of the right to private life, and the criterion whether the interference is necessary in a democratic society, one has to look at the explicit goals of the proposal. The aim is according to the text of the current proposal the "prevention, detection, and investigation of terrorist offences and other serious criminal offences". These goals are absolutely different from the goals for which Eurodac has been established. Even if these goals can be gathered under the purposes mentioned in Article 8 (2) ECHR, "interests of national security", and even "prevention of disorder and crime", this does not automatically imply that the intended access to Eurodac information is "necessary in a democratic society". This criterion requires that the intended measure is both proportionate and subsidiary with regard to the interference with the individual right. The Meijers Committee concludes that the current proposal lacks sufficient evidence on its necessity and proportionality. In the Commission Communication on enhanced interoperability and synergies among EU databases (COM (2008) 825), the absence of the possibility for law enforcement authorities to access to Eurodac was only reported as a "shortcoming", without further evidence. The impact assessment accompanying the current proposal provides only marginal information on the usefulness and proportionality of the measure. The Commission refers to data from only four Member States (p. 8) concerning the hit rates in cases where the national law enforcement authorities used data files with fingerprints of asylum seekers. These data provide insufficient and outdated evidence of the necessity to give law enforcement authorities and Europol access to the Eurodac data on asylum seekers as these data do not provide any systematic analysis of the causal relationship between the availability of data on asylum seekers on the one hand, and the prevention, detection or investigation of terrorist offences and other serious criminal offences on the other hand.

This conclusion applies, for example, to the information of the Commission that according to statistical data in Germany in 2006, 19,4% of the crimes were committed by non-nationals of which 8,5% were asylum seekers. Irrelevant is also the addition that according to these German statistics, of all types of crimes committed by non-nationals 28% related to homicide and manslaughter, and of this 28%, asylum seekers committed less than 14%! Also the information from the Dutch government that between September 2004 and January 2006 consultations on the databases with fingerprints on aliens, including fingerprints on asylum seekers produced a hit rate of more than 44% is insufficient for the conclusion that therefore information on asylum seekers stored into Eurodac must be accessible for national law enforcement authorities of EU Member States and Europol. The Commission also refers to data provided by the Austrian government according to which in 2006, 19% of recorded *crime suspects* would have been asylum seekers, however without taking into account numbers on asylum seekers who were actually *convicted* for those crimes. The same problem applies to the data provided

by UK authorities according to which between 2007 and 2008 consultation on the Immigration and Asylum Fingerprint System including fingerprints on asylum seekers produced a hit rate of 7% on counter terrorism: no evidence is given on the number of asylum seekers who were actually prosecuted or convicted for terrorist crimes.

In *Marper v. UK* judgment, the ECtHR emphasized that such statistics are insufficient to justify the indefinite and extended registration of fingerprints and DNA for law enforcement purposes. In this case, the ECtHR was asked to consider the relevance of statistics provided by the UK Government to justify their retention of fingerprints and DNA of the applicants. Where the applicants asserted that the statistics provided by the UK government as justification for the retention of the data were misleading, the ECtHR affirmed that the figures did not reveal “the extent to which the “link” with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons” (para 116). Nor did they, according to the ECtHR, demonstrate that the high number of successful matches with crime-scene stains was only made possible through indefinite retention of DNA records of all such persons. Therefore, the statistics in themselves did not establish that the successful identification and prosecution of offenders could not have been achieved by other means than the permanent and indiscriminate retention of fingerprint and DNA records (para. 117). Even if the extension of databases contribute to the detection and prevention of crime, the ECtHR emphasized that the question remained whether “such retention is proportionate and strikes a fair balance between the competing public and private interests” (para. 118).

Considering the right to privacy under Article 8 ECHR, the ECtHR emphasized in the *Marper v. UK* judgment the right of every person to be presumed innocent. According to the ECtHR, even if the retention of private data on a person cannot be equated with the voicing of suspicions, nonetheless their perception that they are not being treated as innocent could be heightened by the fact that their data are dealt with in the same way as convicted persons (para. 122). Considering the special position of asylum seekers and even the position of their relatives in the country of origin, see further below, the Meijers Committee concludes that the Commission failed to make a fair balance between the interests of law enforcement authorities and those of the asylum seekers.

Furthermore, the current proposal does not fulfil the principle of subsidiarity under Article 8 (2) ECHR. According to the Commission, without any action at EU level “law enforcement authorities will continue to remain ignorant whether or not information on a fingerprint is available at all and in which Member State”, without giving convincing evidence why measures such as the Prüm Decision and the Framework Decision 2006/960 do not fulfil the necessary requirements for an effective cooperation. On the contrary, by concluding that these measures would not work, because this requires the launching of “29 requests for mutual legal assistance with the aim of discovering which, if any, Member State holds data in relation to a fingerprint” which would be a “hypothetical process”, the Commission seems to question the efficiency of these EU instruments for the protection of security and for law enforcement purposes in general. The question arises whether the efficiency of existing measures should not be evaluated before adopting new measures such as the proposed extended use of Eurodac.

#### *In accordance with the law*

With regard to the criterion “in accordance with the law”, it is not sufficient for the interference with the right to private life to have some basis in domestic law: the law must be accessible to the individual and its consequences must be predictable. Firstly, the provisions in the aforementioned draft of Article 3 do not provide clear and predictable criteria on the basis of which an asylum seeker may be aware that his fingerprints, initially provided for administrative purposes only, may be transferred to national authorities of 30 Member or Contracting States and to the European organisation, Europol. Secondly, the Eurodac proposal only provides that the Member States will appoint “designated authorities” gaining access to the Eurodac data, without giving any definition or limitation of those authorities. It is clear that for an individual asylum seeker coming from a country outside the legal system of the 30 States using Eurodac, it is simply impossible to find out which authority in which country may, under certain circumstances get access to his or her personal information. The provision in the Eurodac proposal, stating that the Member States will make lists of “designated authorities” and send these lists to the European Commission, is in this regard an insufficient safeguard. This will allow Member States to appoint different national authorities having access to the data on asylum seekers in

Eurodac. As a result, comparable with the use of the Schengen Information System and the Visa Information System, Eurodac will be accessible by a large number of authorities within the European Union and the aforementioned third states. This large number of “designated authorities” will hamper the effective control on the use and further storage of the fingerprints of asylum seekers.

### **3 Right to data protection – purpose limitation**

According to the Commission, in the explanatory memorandum to the draft Regulation, the current proposal would be “fully in line with the Charter of Fundamental Rights, and more specifically, the protection of personal data in Article 8. This conclusion is merely based on the conclusion that Directives 95/46 and Regulation 45/2001 apply to the processing of personal data carried out under the Regulation and the Framework Decision 2008/977 apply to the processing of personal data carried out by law enforcement authorities. The Meijers Committee notes that with this conclusion, the European Commission establishes a very minimalist view of the right to data protection and the obligations deriving from the Directive 95/46. As we have stated in previous comments on the proposed use of Eurodac for law enforcement authorities, this extended use violates the principle of purpose limitation as included in Article 6 and 7 of the EC Directive 95/46. For this reason the current proposal if adopted risks annulment by the ECJ. In the judgment *Rechnungshof v. Österreichischer Rundfunk*, the ECJ explicitly stated that EC Directive 95/46 must be interpreted in accordance with the right to private life as protected in Article 8 ECHR.<sup>2</sup> According to the ECJ, if national courts were to conclude that the national legislation with regard to the processing of personal data is incompatible with Article 8 of the Convention, that legislation would also be “incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46” (para. 91). Furthermore, it considered that the principles and criteria for legitimate data processing (as laid down in Articles 6 and 7 of the Directive, so including the purpose limitation) have a direct effect, in the sense that an individual may seek access to a national court in order to prevent the application of national rules contrary to these principles (para. 100). In this regard it is important to underline that purpose limitation implies that data processing should be foreseeable for the data subject and should not go beyond the reasonable expectations of the person concerned.

The importance of a strict reading of the purpose limitation principle also follows from the judgment of the ECJ in the case *Huber v. Germany* dealing with the registration of an Austrian citizen, Mr. Huber, in the German central aliens administration or AZR.<sup>3</sup> In this judgment the ECJ held that the storage of information on EU citizens in the national aliens administration to support national authorities responsible for the application of the law relating to the right of residence can be considered to satisfy the requirement of necessity laid down by Article 7(e) of EC Directive 95/46, interpreted in the light of the prohibition on any discrimination on grounds of nationality, as long as:

- it contains only the data which are necessary for the application by those authorities of that legislation, and;
- its *centralised* nature enables the legislation relating to the right of residence to be more effectively applied as regards Union citizens who are not nationals of that Member State.

With regard to the use of the aliens administration for law enforcement purposes, the ECJ held that the putting in place by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State was not compatible with the prohibition of discrimination as included in Article 12 EC. Furthermore, the ECJ explicitly referred to the duty of the national authorities of Member States to guarantee the accuracy and relevancy of the data being stored “since a change in the personal situation of a party entitled to a right of residence may have an impact on his status in relation to that right, it is incumbent on the authority responsible for a register such as the AZR to ensure that the data which are stored are, where appropriate, brought up to date so that, first, they reflect the actual situation of the data subjects and, secondly, irrelevant data are removed from that register.”

The conclusions of the ECJ in the *Huber* case must be in the first place read against the background of the right to freedom of movement of an EU citizen in another EU Member State, and the prohibition of discrimination included in Article 12 EC. However, there is no reason to conclude that the ECJ will

---

<sup>2</sup> *Rechnungshof v. Österreichischer Rundfunk and Others*, 20 May 2003, Joint Affairs C-465/00, C-138/01 and C-139/01.

<sup>3</sup> C-524/06, 16 December 2008.

apply less strict criteria with regard to asylum seekers: their rights are also protected under EC law, they form a particular vulnerable group (see section 3 below), and the misuse of their personal data may have consequences for their safety and the safety of their family members in their country of origin. Therefore, considering the aforementioned criteria formulated by the ECJ, it should be taken into account that access by law enforcement authorities to Eurodac, implies the risk that data on asylum seekers in this database which are to be deleted according to the rules of the Eurodac Regulation will remain to be stored by national authorities. Once again, the Meijers Committee underlines that no further control is possible with regard to the unlawful storage of these data and that the current practices of national authorities with regard to the deletion of data from Eurodac establishes that it is difficult to delete the data in accordance with the rules of the Eurodac Regulation. Finally, there is no evidence that in the Member States have reliable mechanisms assuring that asylum seekers who obtained the status of refugee, were issued a residence permit, or were naturalised are automatically deleted from Eurodac, as is required in the Eurodac Regulation.

#### **4 Right to asylum and right to protection against torture and inhuman treatment**

As in its earlier comments, the Meijers Committee emphasizes the special *vulnerable position* of asylum seekers and the necessity of preventing national officials of their countries of origin to get access to information on their asylum applications. Extension of the use of data in Eurodac to other authorities not dealing with asylum application implies the risk that this information will be accessible by other, foreign, authorities as well. According to the Meijers Committee this use is in violation of the right to asylum as protected in Article 18 of the EU Charter on Fundamental Rights. It should be emphasized that the registration of fingerprints in Eurodac is *not voluntary*: each person applying for asylum in one of the EU Member States is obliged to submit his or her fingerprints.

Moreover, 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.

According to Article 3 ECHR, protection against torture or inhuman treatment is absolute regardless of any consideration of public policy or security<sup>4</sup>. 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 far wider range of authorities in Member States who have no experience with the specific risks of asylum related information. This risk has been acknowledged by the European Commission in his explanatory memorandum, however, according to the Commission the current proposal would provide sufficient guarantees, because it prohibits the further transfer of the asylum seekers data to third countries. Considering the different bilateral agreements between EU Member States or Europol and third states, the Meijers Committee has serious doubts about the practical meaning of this prohibition in the current proposal. The way in which the national authorities will use Eurodac information is uncontrollable. Furthermore, 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, could already impede an asylum seeker to apply his or her right to ask for asylum or subsidiary protection.

#### **5 Stigmatisation and discrimination of asylum seekers – 14 ECHR**

Article 14 ECHR obliges Member States to secure the enjoyment of the rights and freedoms as protected in the ECHR without discrimination on any ground such as sex, race, color, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. Aside from Article 14 ECHR, Protocol no. 12 to the ECHR includes a general right protecting the “enjoyment of any right set forth by law” without discrimination on the

---

<sup>4</sup> See for instance the *Chahal* judgment, ECtHR 25 October 1996, app. 70/1995/576/662, para. 106

aforementioned grounds.<sup>5</sup> Different from Article 8 EC Directive 95/46 with regard to the protection of special categories of data, Article 14 ECHR does not include a limitative list of forbidden discriminatory grounds. Considering the special sensitive position of asylum seekers and the fact that Article 14 CHR explicitly refers to “other status”, it must be concluded that the exclusive storage (and use for law enforcement purposes) of fingerprints of individuals who apply for asylum in one of the EU Member States is contrary to Article 14, jo. 8 ECHR.<sup>6</sup> Furthermore, the Committee on the Elimination of Racial Discrimination (CERD) has stated in the preamble of the General Recommendation no. 30 on Discrimination Against Non- Citizens that: “Noting that, based on the International Convention on the Elimination of All Forms of Racial Discrimination and general recommendations XI and XX, it has become evident from the examination of the reports of States parties to the Convention that groups other than migrants, refugees and asylum-seekers are also of concern, including undocumented non-citizens and persons who cannot establish the nationality of the State on whose territory they live, even where such persons have lived all their lives on the same territory” (underlining Meijers Committee).<sup>7</sup>

As argued before by the Meijers Committee on the basis of national jurisprudence<sup>8</sup> as well as the aforementioned ECtHR judgment in *Marper v. UK*, the use of fingerprints of asylum seekers for law enforcement purposes, will lead to *stigmatisation and discrimination* of this group of individuals. The fact that by this extended use of their information, asylum seekers are automatically considered as suspected persons, will influence the way this group of persons will be treated in society as well.

## **6 Conclusion**

To conclude, the Meijers Committee finds that the intended proposal giving law enforcement authorities and Europol access to Eurodac violates fundamental rights of 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 violation of the principle of non discrimination. When adopted, there is a serious risk that these instruments (the proposed Decision and Regulation) will invoke preliminary questions by national courts and subsequently will be held unlawful by the European Court of Justice considering recent jurisprudence of both the European Court of Justice and the European Court for Human Rights. The Meijers Committee advises the members of the European Parliament to vote against this legislative proposal of the European Commission.

o-0-o

---

<sup>5</sup> CETS no. 177, this protocol entered into force on 1 April 2005.

<sup>6</sup> That asylum seekers as «a group» is also to be considered as a forbidden ground of discrimination has been confirmed by the Dutch highest court Hoge Raad: HR 13-06-2000, LJN AA6191 and HR 08-06-2004, LJN AO8326.

<sup>7</sup> General recommendation no. 30 of 1 October 2004, <http://www.unhchr.ch/tbs/doc.nsf/0/e3980a673769e229c1256f8d0057cd3d?Opendocument>.

<sup>8</sup> Judgment of the Bundesverfassungsgericht, 4 April 2006, 1 BvR 518/02 published on 23 May 2006.