

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 10.9.2009
SEC(2009) 937

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Amended proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]

(Recast version)

and to the

Proposal for a

COUNCIL DECISION

on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes

SUMMARY OF THE IMPACT ASSESSMENT

{COM(2009) 342 final}
{COM(2009) 344 final}
{SEC(2009) 936}

1. PROBLEM DEFINITION

The conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 considered that, in order to fully achieve the aim of improving security and to enhance the fight against terrorism, access under certain conditions to 'Eurodac' should be granted to Member States' police and law enforcement authorities, as well as Europol, in the course of their duties in relation to the prevention, detection and investigation of terrorist offences and other serious criminal offences. It therefore invited the Commission to present as soon as possible the necessary proposals to achieve this aim.

The absence of the possibility for law enforcement authorities to access 'Eurodac' to combat terrorism and other serious crime was also reported as a shortcoming in the Commission Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 24 November 2005¹.

'Eurodac' is a Community-wide system for the comparison of the fingerprints of asylum applicants. It was established by the 'Eurodac' Regulation which came into force on 15 December 2000 and which serves all the States that implement the Dublin *acquis*. The purpose of 'Eurodac' is to facilitate the application of the Dublin Regulation², which is aimed at establishing a clear and workable mechanism for determining responsibility for asylum applications, to prevent asylum shopping and to guarantee effective access to relevant procedures. This purpose is achieved by a system of fingerprint identification of third country nationals who fall under the scope of the Regulation under strictly defined and harmonised rules in relation to the storage, comparison and deletion of fingerprints.

The database contains only the following information: the fingerprints, the Member State of origin, place and date of application for asylum, sex, the reference number used in the Member State of origin, the date on which fingerprints were taken and the date on which they were submitted to the Central Unit.

In law enforcement, while Member States successfully access asylum seekers fingerprints on a national level, it seems that access to asylum seekers fingerprint databases of other Member States is more problematic.

Even though there are currently some EU instruments that permit consultation of fingerprints and other law enforcement data held by one Member State by another Member State, a *structural information and verification gap* was identified as regards cross-border exchange of data of asylum seekers, which results in *timely and burdensome procedures* for such cooperation.

The structural information and verification gap is identified in the fact that currently no single system exists that is accessible to law enforcement authorities which enables to determine the Member State that has information on an asylum seeker. If a query of a national AFIS using the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision) does not result in a "hit", it is not certain that no information is available in a Member State. Therefore, law enforcement authorities will not only remain ignorant about whether or not information is available at all and in which Member State, but often also whether this information relates to the same person. Law enforcement officials will only know whether information is available

¹ COM(2005) 597, p. 6.

² OJ L 50, 25.2.2003, p. 1.

in a database of another Member State if their judicial authorities issue a request for mutual legal assistance requesting the other Member States to query their databases and send the relevant information under the Convention on Mutual Assistance in Criminal Matters³. Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities (FWD 2006/960) could only be used when the Member States which holds the data of an asylum seeker is known.

Cooperation is further hampered by the fact that current instruments do not make it possible to exchange such information in a timely and non-burdensome manner. If a Prüm search does not produce a hit, the only available choice for a Member State is to issue mutual legal assistance requests to all other Member States. Without efficient means to determine whether or not information is available in another Member State the action of public authorities becomes prohibitively expensive, is time consuming and hence seriously jeopardises the application of the law. Timely availability of information is particularly relevant to avert harm to persons or goods, or to prevent damage to critical infrastructures. Rapid access is also necessary to forestall destruction of evidence of a serious crime or attempt to commit a serious crime.

2. ANALYSIS OF SUBSIDIARITY

The right of the EU to act in this field is enshrined in Title VI of the Treaty on European Union on Police and Judicial Cooperation in Criminal Matters. The current EU instruments on police cooperation are insufficient to facilitate cooperation between Member States in consulting and exchanging fingerprints of asylum seekers. Without appropriate measures at an EU level, law enforcement authorities will not be able to overcome the existing structural information and verification gap.

Cross-border crime is increasing and presents one of the most serious threats to our society as reported by Europol. Without adequate and efficient cooperation between law enforcement authorities of Member States, including access to relevant information held in other Member States, it will be very difficult, if not impossible, for these authorities to fight such cross-border crime effectively. Because of the very nature of these crimes, instruments on an EU level are required to set the ground for cooperation between Member States.

In addition, action at the EU level will help to ensure harmonised provisions on safeguarding data protection, whereas if Member States are left to legislate independently, a harmonised level of safeguards will be difficult to achieve.

Even though the potential number of asylum seekers that might be involved in cross-border terrorist offences or other serious criminal offences might not be very large, the mere fact of the gravity of such offences and their impact on society and every day life should provide adequate justification for action on an EU level.

3. OBJECTIVES OF THE INITIATIVE

The general objectives:

- The prevention, detection and investigation of terrorism and other serious crime
- The protection of victims of terrorism and other serious crime.

³ Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the convention on mutual assistance in criminal matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 1).

Specific objectives:

- Increasing security in the EU by facilitating the verification of the identity of certain categories of third country nationals and closing the structural information gap and by ensuring timely and less burdensome procedures for verification of the identity of such persons.
- Facilitating the identification of victims using the same means.

The above policy objectives should be pursued while ensuring that fundamental rights are always protected, especially the right to asylum and the right to protection of personal data, by imposing conditions and safeguards for the access.

4. POLICY OPTIONS

4.1. Refraining from addressing the issue on an EU level – Maintaining the status quo (Policy Option A)

This policy option entails no action to be taken by the EU. The identification and verification processes would therefore remain lengthy; the procedures would remain disproportionately burdensome and their outcome would remain uncertain.

4.2. Regulating the access to 'Eurodac' for law enforcement purposes (Policy Option B)

This policy option establishes the basis for conditional access by Member States' law enforcement authorities as well as Europol to 'Eurodac' on the basis of an amendment of the 'Eurodac' Regulation and by regulating the actual access and use of the personal data held in 'Eurodac' in an accompanying proposal for a Council Decision. A hit reply would be accompanied with the types of data contained in 'Eurodac'. Requests for supplementary information following a hit would not be regulated in the proposed Council Decision but rather be covered by existing instruments, like the FWD 2006/960 and mutual legal assistance.

There are 2 possible sub-options: (i) to provide search possibilities of 'Eurodac' merely on the basis of fingerprints, or (ii) on the basis of fingerprints and latents. Currently, 'Eurodac' does not provide the possibility of searching on the basis of latents and this feature would have to be added on the 'Eurodac' system. However, searching on the basis of latents is a fundamental function for law enforcement cases, where in crime scenes there is usually only the possibility to recover latents.

4.3. Regulating the access to 'Eurodac' for law enforcement purposes as well as the exchange of supplementary information on asylum seekers (Policy Option C)

This policy option establishes the basis for conditional access by Member States' law enforcement authorities as well as Europol to 'Eurodac' on the basis of an amendment of the 'Eurodac' Regulation and by regulating the actual access and use of the personal data held in 'Eurodac' in an accompanying proposal for a Council Decision. A hit reply would be accompanied with the types of data contained in 'Eurodac'. The proposal would also establish a specific process whereby, following a hit, the requesting Member State can request supplementary information from the Member State of origin about the asylum seeker to whom the fingerprint belong, rather than making such a request using existing instruments as in the case of Policy Option B.

There are 2 possible sub-options, as in the Policy Option B: (i) to provide search possibilities of 'Eurodac' merely on the basis of fingerprints, or (ii) on the basis of fingerprints and latents.

4.4. Regulating access to national data about asylum seekers for law enforcement purposes (Policy Option D)

This policy option would create a decentralised network mechanism that would allow each Member State to search the national asylum seekers databases of all the other Member States in an automated manner. Member States should provide for separate national databases which would be used only for law enforcement, as well as for a separate mechanism to network the databases of all the Member States together. This new network would model the content of the data that is recorded in 'Eurodac' as well as the functions of 'Eurodac' itself. This model would be similar to the search hit/no hit model that was established by the Prüm Decision. Access to supplementary information would be achieved by special provisions in the Eurodac Decision or by using existing instruments.

The costs of this policy option would be disproportional. It would entail the creation of special databases in each Member State and the setting up of a complicated network that would connect these databases of all Member States together. It would seem unnecessary and inappropriate to create an entirely new, complicated technical architecture for the only reason to enable law enforcement authorities to search for information already held in an existing database. For these reasons, this policy option is not considered proportionate and is dismissed at this point.

5. ASSESSMENT OF IMPACTS

The impacts of the proposed policy options are assessed under the following criteria:

- Increasing security in the EU by facilitating the verification of the identity of certain categories of third country nationals and closing the structural information gap.
- Increasing security in the EU and facilitating the identification of victims by ensuring timely and less burdensome procedures for verification of the identity.
- Fundamental rights impacts, impact on the right to asylum and to the protection of personal data.
- Implementation costs for Member States' administrations.
- EU budget.

Policy Options B and C would have an equivalent great positive impact in increasing security in the EU and the same impacts on fundamental rights. However, the two Policy Options differ as regards implementation costs for Member States' administrations, with Policy Option C being more expensive. Policy Option C would entail additional costs for creating a new administrative and technical architecture for the exchange of the supplementary information. Such costs may be considerable, since Member States need to ensure that the additional information has to be made available within a certain timeframe. It will also be necessary to ensure timely availability in cases of urgencies.

6. COMPARISON OF OPTIONS

The "no action" policy option does not improve security in the EU. Maintaining the status quo would mean that law enforcement authorities will continue to remain ignorant about whether or not information on a fingerprint is available at all, in which Member State information is available, and whether information relates to the same person, and will remain unable to obtain such data. The alternative of requesting hypothetical mutual legal assistance from all Member States is too timely and too burdensome to present a realistic option.

The Policy Options B and C on introducing the necessary proposals to allow access to 'Eurodac' by law enforcement authorities possess a clear advantage in that they assist in increasing security in the EU, by facilitating the verification of the identity of certain third country nationals and closing the structural information gap, ensuring timely and less burdensome procedures for verification of the identity of such persons and ensuring the possibility to search 'Eurodac' on the basis of latents.

Even though the achievement of the objectives would be more effective under Policy Option C than Policy Option B, it is considered that the costs of implementing Policy Option C would be high in relation to Option B. In addition, currently there are no indications that FWD 2006/960 would not be a sufficient instrument for the exchange of supplementary information.

Policy Option B would still render the exchange of supplementary information possible and simple, while respecting the exceptions and conditions that are in place about the general exchange of law enforcement information. There seems to be no reason to create special rules to regulate the exchange of information on asylum seekers. Furthermore, there seems to be no reason for which a new (costlier) organisational and technical architecture is established for the exchange of the supplementary information, when current systems are adequate and appropriate for this purpose. It is the preferred policy option.

This policy option could have several sub-options. The choice between these sub-options is not made in this impact assessment and is left to the political decision makers.

One such sub-option relates to the scope of the instrument. The scope would be limited to the prevention, detection and investigation of terrorist and other serious criminal offences. It is being suggested that the term "serious criminal offences" could refer: (i) to the list of serious criminal offences as described in the European Arrest Warrant Framework Decision, as per the preference of the Member States, (ii) it could be a more limited list of offences which would be adopted specifically for this instrument and which would exclude any kind of crime which might be specifically relevant to asylum seekers, like illegal entry, as per the preference of the civil liberties experts, or (iii) it could be the list of crimes of the European Arrest Warrant with some special guarantees for crimes specifically relevant to asylum seekers.

Another sub-option could relate to the type of public authorities that could have access to the 'Eurodac' data. Such authorities should be authorities responsible for the prevention, detection and investigation of terrorist offences and serious crime. The designation of such authorities could be (i) totally at the discretion of the Member States, or (ii) subject to the approval by the Commission. In the latter case the Member States should inform the Commission.

A third set of sub-options relates to the duration of the instrument. The core difference between the three sub-options is whether or not they include a time-limit (sunset clause) and, if so, the duration of that limit.

7. MONITORING AND EVALUATION

Each Member State will carry out annual evaluations of the effectiveness of consulting 'Eurodac' and the Commission will review the operation of the access to Eurodac after five years from its entry into force and submit a report to the Council.