COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 10.9.2009
SEC(2009) 936

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

IMPACT ASSESSMENT

{COM(2009) 342 final}
{COM(2009) 344 final}
{SEC(2009) 937}

TABLE OF CONTENTS

PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

Impact Assessment Board

On 18 March 2009, the Impact Assessment Board of the European Commission delivered an opinion regarding a preliminary version of this Impact Assessment report. According to the IA Board the IA report provides a clear overview of the possibilities and limitations of existing EU instruments which permit consultation of fingerprints and other law enforcement data held in another Member State. In their opinion the IAB in brief stated also that the report should be further improved by better illustrating the necessity and proportionality the proposed measures.

It further stated that:

- The access to other databases by law enforcement should be better explained.
- The potential relationship with the Prüm Council Decision should be further examined.
- The impacts on national data protection provisions should be further clarified.

The present version of the Impact Assessment report has been significantly redrafted, with a view to taking these recommendations fully into account. Additional information and modifications have been introduced to this end in many of its sections.

Consultation and expertise

For the purpose of the preparation of this report, the Commission sent out a questionnaire in July 2007 to the States applying the Dublin *acquis*, i.e. the Member States, Iceland, Norway and Switzerland (for the purposes of this Impact Assessment all these States will be referred to jointly as 'the States that implement the Dublin *acquis*'), as well as to Europol. The questionnaire aimed at examining the necessity, possible modalities and conditions to consult 'Eurodac'.

In addition, the Commission organised three meetings with different categories of stakeholders in order to discuss the issue further.

First, the Commission invited representatives of the States that implement the Dublin *acquis* and Europol to an expert meeting in Brussels on 25-26 September 2007, during which the experts had the opportunity to clarify the replies to the questionnaire and express further views.

Secondly, the Commission consulted the following intergovernmental organisations, non-governmental organisations and other scientific experts working in the area of asylum

law/policy, fundamental rights and protection of personal data during a meeting in Brussels on 8 October 2007:

- Amnesty International
- Centre for European Policy Studies (CEPS)
- Centre for Migration Law
- Council of Europe
- European Council for Refugees and Exiles (ECRE)
- European Liberty Security Organisation (ELISE)
- European Policy Centre (EPC)
- Human Rights Centre, University of Essex
- International Committee of the Red Cross (ICRC)
- International Organisation for Migration (IOM)
- Privacy International
- Standing Committee of experts on international immigration, refugee and criminal law, Netherlands
- The Odysseus Academic Network of Legal Studies on Immigration and Asylum in Europe, represented by Mr Jens Vedsted-Hansen, co-editor of European Journal of Migration and Law.

Representatives of the LIBE Committee of the European Parliament, more particularly Jean-Marie Cavada, Ewa Klamt and Baroness Sarah Ludford also participated at the same meeting.

Finally, the Commission consulted representatives of the national data protection authorities of the States that implement the Dublin *acquis*, as well as the Joint Supervisory Body of Europol and the European Data Protection Supervisor during a meeting held in Brussels on 11 October 2007.

A steering group has been set-up for the specific purposes of this report. The group consisted of officials from the various Directorates of DG JLS, DG RELEX, SG and SJ it met once on 30.01.2009 to discuss the issue and further comments where provided in writing. A steering group was also convened at an earlier stage to consider wider matters arising from the 'Eurodac' Regulation, some of which were elaborated within the context of the Impact Assessment on the revision of the 'Eurodac' Regulation[1]. with the participation of DG RELEX, SANCO and EAC and met on 20.06.2008.

[1] SEC(2008)2981

On 20 October 2008 an additional questionnaire was sent out to the Member States. This was aimed at receiving updates to the replies to the initial questionnaire and at clarifying issues that were not raised in the initial questionnaire but were raised during the expert meetings.

Annex 1 contains a compilation of the replies to the questionnaires and Annex 2 is a report of the observations made by the experts in the all the above expert meetings that were convened in 2007.

PROBLEM DEFINITION

The context

The Hague Programme[2] stated that the exchange of information to strengthen security should be improved. One of the ideas contained in the Programme is to make full use of new technology, *inter alia* - where appropriate – by direct (on-line) access for law enforcement authorities, including for Europol, to existing central EU databases.

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 2005[3].

Council Regulation (EC) No 2725/2000 of 11 December 2000 established 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention[4] (the 'Eurodac' Regulation). On 3 December 2008 the Commission adopted a proposal to amend the 'Eurodac' regulation, which is accompanied by an impact assessment[5]. That proposal is aimed at making the 'Eurodac' system more efficient.

'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 Community-wide information technology system for the comparison of the fingerprints of asylum seekers started operations on 15 January 2003.

---

2 OJ C 53, 3.3.2005 p.7/8.
3 COM(2005) 597, p. 6.
4 OJ L 316/1 of 15 12 2000
5 COM(2008) 825 final and SEC(2008) 2981 respectively.

The purpose of 'Eurodac' is to facilitate the application of the Dublin Regulation[6], 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. Strict data protection rules are also laid down in order to protect the fundamental right to the protection of personal data.

The 'Eurodac' Regulation established a **Central Unit** managed by the European Commission containing an Automated Fingerprint Identification System (AFIS), which receives data and transmits "hit – no hit" replies, i.e. replies which indicate whether in fact the 'Eurodac' database contains the specific fingerprint, to the national Units in each Member State. The Central Unit processes the fingerprints of the following types of data on individuals over the age of 14 as follows:

Category 1 (CAT1): data of asylum applicants are *sent for comparison* against fingerprints of other asylum applicants who have previously lodged their application in another Member State. The same data will also be compared against the "category 2" data. This data will be *stored* for 10 years;

Category 2 (CAT2): data of aliens apprehended in connection with the irregular crossing of an external border and who were not turned back. These data will be sent for *storage only*, in order *to be compared against* data of asylum applicants submitted subsequently to the Central Unit. This data will be kept for two years;

Category 3 (CAT3): While the storage of the two above is compulsory under the Regulation, the Member States themselves can decide (i.e. *transmission is optional*), whether they wish to use the facility of the CAT3 comparison (transmit fingerprints taken from aliens found illegally present in a Member State) to determine whether the person in question is in fact an asylum seeker in one of the Member States. CAT3 data are not stored, but are only searched against the data of CAT1 stored in the central database.

For those categories that are stored, 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.

[6] OJ L 050, 25.02.2003, p.1

On 31 December 2008, 'Eurodac' contained 1.221.208 sets of fingerprints of asylum seekers and 102.155 data sets of persons apprehended in connection with an irregular crossing of the external border. The 'Eurodac' system was designed to be capable of storing 800.000 full ten print images and is currently capable of storing 1.600.000 ten print images. This shows that it has not yet reached the upper limit of its storage capacity.

The total of successful transactions sent to the Central Unit in 2008 totalled 357.421, i.e. an average of 979 per day. The system is designed to process 3.750 transactions per day. The number of transactions of data of asylum seekers (CAT1) was 219.557. In addition, 61.945 transactions were sent in as CAT2.

Description of the problem

Information about citizens of EU Member States and about third country nationals is available in many forms and systems in the Member States and at EU level. National and European instruments lay down the rules and conditions under which law enforcement authorities can have access to this information in order to carry out their lawful tasks.

Fingerprint data is especially useful information for law enforcement purposes, as it constitutes an important element in establishing the exact identity of a person. The usefulness of fingerprint databases in fighting crime is a fact that has been repeatedly acknowledged.

The European Union has adopted several legislative instruments under which fingerprint data may be consulted by law enforcement authorities of Member States. These systems provide law enforcement officials either with detailed information about an individual and visa data related to him/her (the Visa Information System), or with an indication for which reason an individual is wanted by a national authority and the action to be taken in a concrete case (the Schengen Information System), or with a "hit/no-hit" signal, indicating whether further information is available about that person in a given Member State (the information exchange system set up under the Prüm Council Decision).

Fingerprint data of asylum seekers are collected and stored in the Member State in which the asylum application was filed, as well as in 'Eurodac'. The obligation to collect the fingerprints and other data of asylum seeker and to store them in Eurodac stems from the 'Eurodac' and the Dublin Regulations.

Replies to the second questionnaire (Annex 1) were received by 13 States that implement the Dublin *acquis*, 11 of which are Member States. These replies showed that the 6 Member States and 2 other States that implement the Dublin *acquis* keep asylum seekers fingerprints in their general fingerprint databases (AFIS), while 3 Member States keep such fingerprints in databases that contain fingerprints of all aliens, and 2 Member States keep them in special asylum seekers' databases. In all but one States that replied to this questionnaire, the law enforcement authorities had direct access to their national databases that contain the fingerprints of asylum seekers. In one Member States law enforcement authorities had indirect access to such national database, i.e. access following a judicial authorisation. The replies to this questionnaire indicate that law enforcement authorities use asylum seekers fingerprints in the fight against crime as a matter of course and that the use of such data domestically is conceptually established.

During the consultation of experts it became clear that those national law enforcement authorities that consult national databases containing fingerprints of asylum seekers for

criminal investigations consider the hit rate significant. Only a few Member States keep statistics on the use of the data or the hit rate of such consultations, , while the majority does not hold such statistics. Those Member States that keep statistics were able to report the following:

– German law enforcement authorities claimed that the comparison of fingerprints against national databases containing fingerprints of asylum seekers contained a substantial hit rate up to 40%. According to statistical data of the German Federal Police 19,4% of the crimes in Germany in 2006 were committed by non-nationals. 8,5% of the non-nationals were asylum seekers. 28% of all types of crimes committed by non-nationals related to manslaughter and homicide. Asylum seekers committed less than 14% of this proportion.

– According to the Dutch Ministry of Justice, between September 2004 and January 2006 consultations of the Dutch data filing system containing fingerprints of aliens, which includes the fingerprints of asylum seekers, produced a hit rate of more than 44%.

– Austrian statistical data on 2006 demonstrate that over 19% of the crime suspects recorded were asylum seekers. This figure gives however no indication on the success rate of comparing fingerprint data against fingerprints recorded of asylum seekers.

– In the United Kingdom, between 2007 and 2008 consultations of the Immigration and Asylum Fingerprint System, which includes the fingerprints of aliens and asylum seekers, produced a hit rate of 7% on counter terrorism [statistics on serious crime have not been provided].

It should be noted that the types of crimes for which access to fingerprints of asylum seekers is permitted and the modalities of such access differ among Member States. As a result, the statistics provided by the above Member States cannot be compared.

However, while law enforcement authorities of Member States successfully consult asylum seekers fingerprints on a national level, it seems that access to asylum seekers fingerprint databases of other Member States is more problematic. The problem is therefore identified, not in the use of asylum seekers fingerprints for law enforcement purposes, but, contrary to other forms of law enforcement information, in the lack of effective possibilities for law enforcement authorities to cooperate in exchanging such fingerprints.

Structural information and verification gap

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.

The first instrument that is likely to be used for consultations regarding fingerprints is Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision) which will be implemented by Member States by June 2011. On the basis of this Council Decision the Member States' grant each other automated access *inter alia* to national Automated Fingerprint Identification Systems (AFIS) on the basis of a hit/no hit request. If a query on the basis of the Prüm Decision produces a hit, supplementary information, including personal data, can be obtained

in the Member State that recorded the fingerprint in its national AFIS using national law[7], including mutual legal assistance.

While this procedure might be successful for those Member States that store fingerprints of asylum seekers together with other fingerprints collected by law enforcement authorities in a national AFIS, it will be unsuccessful for those Member States that do not store fingerprints of asylum seekers in their national AFIS unless they are related to crime.

Another instrument that could be used for consultations regarding fingerprints is Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities (FWD 2006/960). This instrument facilitates the exchange of information (the fingerprint as well as the supplementary information) that is held or is available to law enforcement authorities in Member States. This instrument is operational as from 18 December 2008.

The use of this instrument is subject to conditions and safeguards. First, information can be requested from a Member State only if there are factual reasons to believe that the information is actually available in that Member State. Therefore, if the requesting Member State does not know which other Member State might hold data on a person, either because it just has a latent[8] from a crime scene or an uncooperative suspect, then it would be impossible to use this instrument failing such factual information. Also, it cannot be envisaged that a Member State sends the same request for information to all other Member States, as it would be impossible to factually justify all such requests.

Second, in some Member States fingerprints of asylum seekers may only be accessed by a law enforcement authority with the agreement or authorisation of a judicial authority. In such a case, the requested law enforcement authority will be obliged to ask the judicial authority for an agreement or authorisation to access and exchange the information sought. In such a case the requested Member State must reply to the request within 14 days, which is still a reasonable timeframe.

Furthermore, it is also possible that in some Member States that have not replied to the second questionnaire national asylum data are not at all available to law enforcement authorities, in which case this instrument could not be used.

The last instrument that Member States could use is mutual legal assistance under which the judicial authorities of the Member States can seek access to criminal and non-criminal fingerprint collections, including on asylum seekers on the basis of the Convention on Mutual Assistance in Criminal Matters[9]. The request should be addressed to all Member States that are believed to have the relevant information (potentially all other Member States). The execution of a request for mutual legal assistance (also known as a rogatory commission) is

---

[7] Such national law could be the national implementing legislation of the Framework Decision 2006/960 on simplifying the exchange of information and intelligence between law enforcement authorities (FWD 2006/960)

[8] Latents, are fingerprint images left on a surface of an object that was touched by an individual at a crime scene.

[9] 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 2000/C 197/01 of 12.7.2000)

onerous and time consuming especially if it cannot be determined beforehand that the person who is the subject of a criminal investigation or who is victim of a serious crime is an asylum seeker. In that case dutifully answering a request for mutual legal assistance requires searching all potentially relevant national databases.

Although currently most Members States do not keep statistics on how many times they had received a request from another Member State using any of the above mentioned existing instruments on whether or not information on a fingerprint was available, those that keep statistics provided replies ranging from 3000 to respectively 3529, 3763 and 6292 requests on an annual basis. It should be noted that these figures were provided by Member States that previously participated in the Prüm Treaty and that used the cooperation mechanisms of that Treaty (Germany, Austria, the Netherlands, Belgium, Luxembourg, France and Spain). It would be impossible to follow-up such a high number of requests on the basis of mutual legal assistance instrument, bearing in mind the lengthy nature of this process.

It should be noted at this point that the Schengen Information System (SIS) and the Visa Information System (VIS) do not contain fingerprints of asylum seekers, unless s/he has applied for a Schengen visa and is therefore stored in the VIS as a visa applicant, or s/he is wanted for arrest or an alert has been issued for the purpose of refusing entry, in which case s/he will be in SIS. If the data of an asylum seeker are already in VIS or SIS, law enforcement authorities will have access to them under current legal instruments. In all other cases the data of an asylum seeker are only in 'Eurodac'.

On the basis of the above, it seems that the current EU instruments are insufficient to facilitate the cross-border consultation of fingerprint data of asylum seekers, and the situation is exacerbated by the fact that the national data is not always held in the same type of databases, while national law does not always and under the same conditions authorise access to such data for law enforcement purposes. Identification is essential for law enforcement authorities to assist them in their mission to prevent and combat terrorism and other serious crime involving third country nationals, as well as to protect a third country national who is a victim of such a crime.

When information is available from different databases but this information cannot be linked to the person who is the subject of the law enforcement action, fingerprint comparison is a reliable means to remove that uncertainty. In particular with regard to asylum seekers, with or without official documents, confusion can exist with regard to the exact spelling of a name and date of birth because of lacking or imprecise registers. Further, in case a person has several names, changed names or is known under nicknames or pseudonyms, the need exists to determine that the fingerprints relate to one and the same person.

The structural information and verification gap is identified in the fact that, even though it is lawful for Member States to cooperate in obtaining data on asylum seekers, from a practical point of view, 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 and therefore from which Member State the information should be requested. If a query of a national AFIS using the 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 in a database of

another Member State if their judicial authorities issue a request for mutual legal assistance requesting the other Member State to query their databases and send the relevant information.

It should also be noted that the identified structural information and verification gap is a problem which is specifically relevant to data of asylum seekers. Data on EU citizens exists in many different databases in Member States which are in general available to law enforcement authorities. Such information that is accessible to the law enforcement authorities of a Member State is, as a rule under current EU laws, accessible to the law enforcement authorities of other Member States. Further, law enforcement authorities of all Member States already have access to the VIS which contains data on all visa applicants. On the other hand, data on asylum seekers exist only in one single database in each Member State, for which the above identified practical cooperation problem exists. It is therefore obvious that, for all categories of people, other than asylum seekers, information exists in ways that it is accessible to law enforcement. In this respect, providing a way of making cooperation in the exchange of such data possible, will correct an imbalance that exist in relation to data of asylum seekers.

Information is not available in a timely and the least burdensome manner

In addition to the structural information and verification gap, cooperation between Member States in the form of exchange of asylum seekers fingerprint data, 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, which is a very time-consuming, burdensome and costly procedure. It involves months of work for both the requesting and the requested Member State, while it involves substantial costs in respect of the staff involved throughout these months, translations, court appearances etc. 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. Moreover, a fast check of the exact identity of a detained suspect is required if there are serious grounds to believe that (s)he is a member of a criminal organisation that is about to carry out a serious crime. Precise information about the identity of the detained suspect increases the chances to identify the other members of the organisation. Such information is also necessary to ensure that criminal investigation focuses on the right person.

Examples

Some examples that have been presented by the consulted national law enforcement authorities that indicate the identified problems are the following:

- A third country national is arrested at the border of a Member State because of suspicion of involvement in a serious crime. In the interview the suspect provides a false identity or generally refuses to provide an identity. Comparison of his fingerprints against national databases and the national AFIS of other Member States using the Prüm Decision are without result. It is not possible to find any information on this person. Mutual legal Assistance requests to all other Member States would not be a practical and proportionate measure. Access to asylum data of other Member States would have provided and identity and have

opened leads for investigation. This would have been beneficial for the investigation and for the prevention of crimes.

- At a crime scene the dead body of a person is found. Investigation shows that the person could have been a third country national. Latents recovered at the crime scene could be those of the murderer. They are compared against national databases and the national AFIS of other Member States using the Prüm Decision but without success. The police is of the opinion that enquiring asylum data on the basis of latents would have been relevant, because both victim and possible murderer could be identified.

- The body of a person is found in a city in a Member State and investigation brings to light that the cause of death was unnatural and probably of criminal origin. No identification papers are found. Ten prints are taken to establish the identity. Consultation of the national databases and the national AFIS of other Member States using the Prüm Decision are without result. The Member State does not have any realistic option to establish the identity of the person. Mutual legal Assistance requests to all other Member States would not be a practical and proportionate measure.

Multiplication of personal data processing

Because currently no single system exists allowing law enforcement authorities to determine the Member State that holds information on an asylum seeker, the only way to find out is to issue a request for mutual legal assistance to each of the other Members States. This inevitable leads to a multiplication of the processing of the personal data of the same person, since a multitude of Member States are asked to query their databases and reply back to the requesting Member State. This in itself is detrimental to the protection of such data.

If Member States are left to legislate data protection independently, a harmonised level of safeguards will be much more difficult to achieve, which may hamper cross-border cooperation between law enforcement authorities as well as create different treatment of personal data because of diverging levels of data protection between Member States. During the discussions in Council on a framework decision on data protection for police and judicial cooperation, it became apparent that on some issues Member States have very different standards and definitions, as for example the case of what is an appropriate data retention period, how far the obligation to inform the data subject applies, i.e. the cooperation between Member States would be hampered when the requested Member State did not inform the data subject of the processing of the data, while the requesting Member State would be obliged to do so. By regulating at an EU level, data protection rules and safeguards can be harmonised, as regards the data that will be made available on the basis of the EU measures. This, in itself, will be a major contribution of action by the EU in this filed.

Europol

The structural information and verification gap as well as the difficulty to obtain information allowing identification in a timely and less burdensome fashion applies to Europol as well. Europol has been mandated to play a horizontal role within the European Union in relation to the fight against cross-border organised crime. In this respect Europol is expected to provide national law enforcement authorities with the necessary tools to exchange information between them, such as exchange of information using the Europol National Units. It follows from the replies of Europol and the Member States to the questionnaire that the exchange of

information between those units would benefit if information exchanged in relation to asylum seekers' fingerprints could form part of the information exchanged to them via Europol as part of a concrete file related to cross-border organised crime. Since Europol currently cannot access information on asylum seekers, it cannot ensure that this information be part of its analysis and investigation tasks.

In addition, it should be noted that Article 28 TEU specifically mentions the cooperation between law enforcement authorities with Europol as one of the main ways to achieve the objectives of police and judicial cooperation in the EU. On this basis, Europol has already been given access to other EU databases, like the VIS and the SIS, while it can also request data which is stored in Member States' national AFIS.

EU right to act and subsidiary principle

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. On the basis of the above analysis, the current EU instruments on police and judicial cooperation are insufficient to facilitate cooperation between Member States in 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 perform their duties in relation to the prevention, detection and investigation of terrorists offences and other serious criminal offences and hence 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. Furthermore, absence of action at EU level would be detrimental for data protection as it compels law enforcement authorities to process much more data than is required if they had access to a central index of available data. In addition, as the safeguards would not be harmonised at EU level, the level of protection of individuals with regard to the protection of their personal data could vary sensibly between Member States. The reason for this is that they have to resort to requests for the data to all Member States, rather than a single request to the relevant Member State. All these requests ultimately lead to the processing of much more data, which itself is detrimental to data protection.

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.

On the basis of the above, it can be concluded that the EU is both entitled to act and better placed to do so than the Member States. Such an action should not go beyond what is necessary to achieve its objectives.

How would the problem evolve, all things being equal?

As already mentioned under section 2.2., the existing instruments do not allow to timely determine with sufficient certainty whether a Member State actually holds fingerprint data of an asylum seeker. This means that without any action at an EU level, 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. Without efficient and reliable means to determine whether or not information is available in another Member State the action of public authorities either becomes prohibitively expensive or seriously jeopardises the application of the law because no further efficient and reasonable action to determine a person's identity can be taken. The reason for this is that the FWD 2006/960 cannot be used in cases where the requesting Member State does not know which other Member State might hold data regarding a particular fingerprint.

Furthermore, there is not a high likelihood that Member States would use the instrument of mutual legal assistance as a way to find out about whether or not information on a fingerprint is available at all in another Member State. In addition, launching 29 requests for mutual legal assistance with the aim of discovering which, if any, Member State holds data in relation to a fingerprint, is a hypothetical process, which inevitably will lead to at least 28 negative replies. The engaging of all the States that apply the Dublin acquis in such a lengthy and burdensome process, which in 28 cases will result in a negative reply, is not an effective way of dealing with the exchange of law enforcement information. Mutual legal assistance was not designed to be used on the basis of hypotheses, but for exchanging data where there is at least a certainty that the requesting Member State holds such information.

POLICY OBJECTIVES

3.1. Objectives

One of the fundamental goals of the European Union is the development of a genuinely European area of justice, freedom and security. Such an area aims to ensure that the fundamental rights of its citizens, such as life, physical integrity, security and the protection of citizens' personal data and privacy, are guaranteed.

The general objectives are:

- The increasing security in the EU by facilitating cooperation between law enforcement authorities of Member States and Europol in exchanging information for the prevention, detection and investigation of terrorism and other serious crime.

- The protection of victims of terrorism and other serious crime.

Such general issues translate into the following specific/operational policy 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;
    - 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.

3.2. Respect of Fundamental rights

The Commission recalls that its legislative proposals in this field have to be compatible with the Charter of Fundamental Rights of the European Union (Charter) and that Member States must respect these rights, when implementing or applying European Union law.

While access to information systems assists law enforcement authorities to prevent, detect or investigate such criminal offences, the collection and processing of fingerprint data must respect other fundamental rights too and must not go beyond what is necessary and proportionate.

The key rights enshrined in the Charter of Fundamental Rights that are engaged here are Article 8 regarding the right to the protection of personal data and Article 18 guaranteeing the right to asylum. The proposed measure would aim to prevent and combat terrorism and serious crime, a legitimate aim that, subject to the principle of proportionality, can justify limitations on

the rights and freedoms recognised by the Charter, provided they are foreseen by law which contain, and respect, the essence of those rights.

The proposed actions would involve a serious interference with the right to the protection of personal data as protected by Article 8 of the Charter on Fundamental Rights of the European Union. The right to data protection may however be interfered with, provided interference is done "in accordance with the law", it is formulated with sufficient precision to allow individuals to adjust their conduct and it protects individuals against arbitrariness and indicates with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. It is also necessary that this interference is "necessary in a democratic society to attain a legitimate and proportionate interest. The jurisprudence of the European Court of Human Rights has decided in various cases that actions aimed at combating terrorism and serious crime, under the umbrella of the exceptions, provided that they are proportionate, and are "in accordance with the law" and "necessary in a democratic society".

The conditions for access to the data would come under the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This Framework Decision contains an explicit reference to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Therefore the measure should comply with the rules on purpose limitation and security of transmissions as well as the other fundamental principles for the lawfulness of data processing activities. The impact on data protection could be reduced by appropriate adherence to the established data protection principles and guarantees. Access should be limited to designated authorities and only on a case-by-case basis. Individuals should be given adequate rights of access, correction and redress in particular the right to a judicial remedy, and supervision of processing operations by public independent authorities should be ensured.

The proposed actions might also interfere with the right to asylum as protected by Art.18 of the Charter. Asylum seekers may be discouraged from applying for asylum as they may know that their personal data may be processed by law enforcement authorities of EU Member States. They could perceive that this could be detrimental to their status or security that, in consequence, could undermine the exercise of their right to asylum. Also, potential asylum seekers may be discouraged from requesting asylum if access to their data is allowed for law enforcement purposes because of fear that such information could end up in the hands of authorities of their country of origin. If such would happen, it could expose relatives or friends of the applicant, or the applicant him or herself to repressions, including the risk of torture or inhuman or degrading treatment. Furthermore, if no alternative destination would be available, it could lead to an increase of undocumented migrants. The measures should therefore include strong guarantees to avoid an interference with the right to asylum, for example by prohibiting the exchange of such data with third countries.

Asylum seekers databases might contain fingerprint data from persons as young as 14 years, but not in all Member States children of this age are criminally responsible. Member States have to ensure that the data of children they retrieve by consulting such databases and which according to their national law cannot be held criminally responsible are treated in a legal and non-discriminatory manner (in comparison to the data from children who are citizens of the concerned Member State) while respecting the principle of the best interests of the child.

POLICY OPTIONS

Under sections 3, 4 and 5 general policy options are presented, assessed and compared. After choosing the preferred policy options, sub-options on more specific provisions will be analysed.

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. In effect this means that no access to 'Eurodac' will be allowed and the information gap will not be filled. The identification and verification processes would therefore remain lengthy; the procedures for identification and verification involving other Member States would remain disproportionally burdensome and their outcome would remain uncertain. No EU intervention means that law enforcement authorities can not swiftly and appropriately identify a person or verify his identity if the Member State that holds these data is not known before a request for information is issued.

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 that are stored 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 Prüm Decision, FWD 2006/960 and mutual legal assistance. In general, FWD 2006/960 requires that the provision of information shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question. To the extent that the FWD 2006/960 cannot be used (i.e. in the case where one of the exceptions of the instrument might apply), then a request for such data could be made using mutual legal assistance. Under the FWD 2006/960, information may be withhold if there are factual reasons to assume that the provision of the information would harm essential national security interests of the requested Member State, jeopardise the success of an investigation or the safety of individuals or clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested. The competent law enforcement authority may also refuse to provide the requested information where the request pertains to an offence punishable by a term of imprisonment of one year or less under the law of the requested Member State. The proposals should contain adequate safeguards to justify the interference with the right to protection of personal data and to guarantee the non-interference with the right to asylum, for example by prohibiting the transfer of such data to any third country.

Access to 'Eurodac' is essential in order to identify the national database that contains additional biographical data of such third country nationals. When 'Eurodac' is searched with fingerprints, it returns, in case the reference set matches a recorded set of ten fingerprints, a hit-reply confirming the match, as well as some additional data. Among the additional data is the reference number that links the fingerprint data with a record held in a separate national database in the Member State that recorded the fingerprint data in 'Eurodac'. The separate file contains further biographical data of the asylum applicant. Access to such additional data is very important for law enforcement purposes. This information usually includes personal

details, identity and travel papers, the members of his family, his former name(s), present and former nationalities, date and place of birth and other information necessary to establishing the identity of an asylum seeker. This additional data should be made available from national files in the case of a hit-reply from 'Eurodac' using existing instruments, as they are usually the only source of biographical information available about asylum seekers.

Based on the analysis in section 3.2, the option should include strong guarantees to avoid an interference with the right to asylum, for example by prohibiting the transfer of the data of an asylum seeker by a Member State to third countries. The policy option will provide appropriate safeguards to ensure the protection of personal data.

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.

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 available types of additional personal data that are stored in 'Eurodac'. The proposal for a Council Decision would also establish a 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 that making such a request using existing instruments as in the case of Policy Option B. The measures should provide the possibility of searching 'Eurodac' on the basis of latents. The proposals should contain adequate safeguards to justify the lawfulness of the interference with the right to protection of personal data and to guarantee the non-interference with the right to asylum.

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.

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

This policy option could have two sub-options:

The first sub-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. To realize this, 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, thus allowing the searches to

happen. 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 sub-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, in particular when a more technically straightforward solution exists, in the form of permitting access to 'Eurodac'. For these reasons, this sub-option is not considered proportionate and is dismissed at this point.

The second sub-option would involve a Recommendation from the EU to the Member States that the Member States should transfer all their asylum seekers' fingerprints in their national AFIS. In this way, Member States would be able to use the Prüm Decision in order to consult the national AFIS of other Member States in order to identify which one holds data relating to a particular fingerprint or latent. Currently, it is at the discretion of Member States to decide in what type of database they will store data on asylum seekers, as well as which authorities might have access to such databases and in what ways. Such a choice usually reflects the national traditions and structures of Member States.

In case that the EU makes a Recommendation to Member States as to where they should store the fingerprints of asylum seekers, it would be interfering unnecessarily with the discretion of Member States on how to set up their national systems. It should be noted that neither the Prüm Decision nor any other instrument harmonise in any way the content of national AFIS.

In addition, the transfer of national fingerprint data to AFIS will be a burdensome and costly exercise which will require changes in national laws as well as modifications of national AFIS to reach new capacity levels and to connect them to the 'Eurodac' system.

This option seems disproportionally complicated and costly and interferes unnecessarily with national systems. For these reasons, this sub-option is not considered proportionate and is dismissed at this point.

5. ANALYSIS OF IMPACTS OF THE POLICY OPTIONS

Table of symbols

small negative impact or small costs	-√
medium negative impact/costs	-√√
Negative impact/costs	-√√√
no impact	0
small positive impact/minor savings	√
medium positive impact/savings	√√
significant impact/savings	√√√

5.1. Policy option A

Policy Option A: Maintaining the status quo		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Increasing security in the EU and facilitating the identification of victims by facilitating the verification of the identity of certain categories of third country nationals and closing the structural information gap	**0**	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. The option does not contribute to increase of security in EU. Maintaining the status quo would imply that the identity of a victim of terrorism or of other serious criminal offence who happens to be an asylum seeker cannot be established.

Policy Option A: Maintaining the status quo		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Increasing security in the EU and facilitating the identification of victims by ensuring timely and less burdensome procedures for verification of the identity	**0**	Without efficient means to determine whether or not information is available in another Member State the action of public authorities becomes prohibitively expensive and seriously jeopardises the application of the law. It would imply initiating potentially 29 requests for mutual legal assistance (i.e. to all other States that implement the Dublin *acquis*), even though the Member State does not even know if another Member State holds or not any data on the fingerprint.
Fundamental rights impacts		
Right to Asylum	**0**	This Policy Option would not authorise any additional law enforcement access to asylum data. However, maintaining the status quo would mean that law enforcement access to asylum data would continue to differ in Member States. Therefore, the direct access to asylum seekers data by law enforcement authorities in some Member States would continue.
Protection of personal data	**0**	This Policy Option would not have any impact on the protection of personal data of asylum seekers since the current situation would remain.

Policy Option A: Maintaining the status quo		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Implementation costs for Member States' administrations	**0**	Maintaining the status quo has no direct financial impact. If the status quo is maintained, then the Member States would be unlikely to take steps to seek the relevant information by launching hypothetical requests for mutual legal assistance. This scenario is considered as the baseline for comparison with other options. The reasons for which Member States are unlikely to resort to mutual legal assistance requests are the complexity and burdensome procedure which ultimately leads to excessive costs. In case that Member States chose to start using mutual legal assistance is all cases, the costs would cover the preparation of a request for mutual legal assistance, the registration and monitoring thereof, the possible translations of the request into the languages of each requested Member State and the registration and the monitoring of the receipt of a reply from the requested Member State and the follow up. The absence of an indication of which Member State should be addressed triggers multiple requests in a single case. According to the replies of the Member States to the questionnaire, the costs could be roughly estimated at three FTE per Member State per year and would be based on the added value of law enforcement officers qualified to process formal requests and law enforcement officers qualified to translate formal requests into the language of the requested Member State and to translate the reply. Based on a estimated hourly wage (average employment costs + 50% overheads) of 25 EUR and 1760 working hours per year (8 hours * 20 days * 11 months) the total yearly personnel costs for all Member States would be 3.828.000 EUR for all Member States. This rough estimation is based on the current level of processing requests per year, and does not take on board any increase in such consultations.
EU budget	0	No impact.

Policy Option A: Maintaining the status quo		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Stakeholders views: Member States/law enforcement	0	Member States expressed consensus that consultation should be allowed for the prevention, detection and investigation of terrorism and other serious crime. Maintaining the status quo does not contribute to enable this, since it would imply that the identity of a victim of terrorism or of another serious crime offence who happens to be an asylum seeker or of a suspect of such a crime cannot be established. Law enforcement stakeholders are of the opinion that access to 'Eurodac' is necessary to achieve an adequate level of efficiency in the prevention, detection and investigation of terrorism and other serious crime. The information contained in Eurodac is required in order to identify which Member State holds information on a fingerprint of an asylum seeker and hence, to establish the identity of a suspect or of a victim. Maintaining the status quo does not contribute to enable this, since it would imply that the identity of a victim of terrorism or of another serious crime offence who happens to be an asylum seeker cannot be established.
Stakeholders views: civil society and data protection	0	Civil society representatives and data protection authorities expressed themselves against granting law enforcement access to 'Eurodac' since such an access in their view would infringe the purpose limitation (asylum and immigration) and change 'Eurodac' into a criminal investigation tool. Maintaining the status quo would not affect the purpose limitation.

Policy Option B

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Increasing security in the EU and facilitating the identification of victims by facilitating the verification of the identity of certain categories of third country nationals and closing the structural information gap	Sub-option (i)√/√√ Sub-option (ii)√√/ √√√	Fingerprint information about third country nationals that are not resident, did not apply for a Schengen Visa and whose data are not for other reasons stored in the Schengen Information System of a Member State is likely only to be found in 'Eurodac' and the national asylum databases. Fingerprint comparison via 'Eurodac' may thus be the only way to establish the identity of such a third country national about whom no other reliable information exists. Fingerprint comparison via 'Eurodac' may be the only way to uniquely identify such a third country national about whom no other reliable information exists. This is essential for law enforcement authorities in order to prevent and combat terrorism and other serious crime involving third country nationals, as well as to protect a third country national who is a victim of terrorism or other serious crime. Access to 'Eurodac' will make it possible to establish the identity of an asylum seeker who is a victim of a terrorist or other serious criminal offence. The establishment of a system of access to 'Eurodac' is also essential in order to identify the national database that contains additional biographical data of such third country nationals. Eurodac' is searched with fingerprints and returns, in case the reference set matches a recorded set of ten fingerprints, a hit-reply confirming the match, as well as some additional data. Among the additional data is the reference number that links the fingerprint data with a record held in a separate national database in the Member State that recorded the fingerprint data in 'Eurodac'. The separate file contains further biographical data of the asylum applicant. Access to such additional data is very important for law enforcement purposes. This additional data from national files should be made available in the case of a hit-reply from 'Eurodac', as they are usually the only source of biographical information available about third country nationals. Existing instruments and channels at national level could be used to make this information available on the basis of European legislation aimed at facilitating the use of those channels. However, this legislation only became operational by the end of 2008, contains some exceptions and the procedures to be used at national level following a hit are only partially harmonised. The search possibility with latents will have a bigger impact since very often it is only possible to recover latents from a crime scene.

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Increasing security in the EU and facilitating the identification of victims by ensuring timely and less burdensome procedures for verification of the identity	√√	Consultation of 'Eurodac' would allow law enforcement authorities to check in minutes where the person involved has applied for asylum. Consulting 'Eurodac' would replace the preparation of individual requests for mutual cooperation and or the querying of 29 databases. The identification of the national database that contains the additional biographical data is especially important since, when law enforcement authorities need to establish the exact identity of a person under investigation, time is a critical factor. In law enforcement what counts is that relevant information is available in a timely, legitimate, secure and cost-efficient manner to assist law enforcement authorities to prevent and combat terrorism and other serious crime as well as to enable them to deal with the victims of such serious crime. The additional biographical information should be made available using existing instruments and channels. Following this procedure for obtaining the additional biographical information would mean not achieving the maximum possible positive impact on security because the exchange of the additional data would still be subject to exceptions. However, currently there are no indications that the main instrument to exchange the supplementary information, FWD 2006/960, would not be a sufficient instrument for the exchange of such information, this instrument being operational only as from 18 December 2008.
Fundamental rights impacts		

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Right to Asylum	-√	Asylum seekers may be discouraged from applying for asylum as they may know that their personal data may be processed by law enforcement authorities of EU Member States and may perceive that this could be detrimental to their status or security which in consequence could undermine the exercise of their right to asylum. Also, potential asylum seekers may be discouraged from requesting asylum if access to 'Eurodac' is allowed for law enforcement purposes because of fear that such information could end up in the hands of authorities of their country of origin. If such would happen, it could expose relatives or friends of the applicant, or the applicant him or herself to the risk of inhuman treatment. Furthermore, if no alternative destination would be available and other conditions would be fulfilled, it could lead to an increase of undocumented migrants. Legislation can counterbalance the risk of such information ending up in the hands of authorities of the applicants home country by prohibiting the transfer of the data of an asylum seeker by a Member state or Europol to third countries. Moreover, rules regarding data security could provide further guarantees against a possible misuse of the data to avoid the data ending up accidently with third countries.

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Protection of personal data	-√√	The proposed actions would constitute a serious interference with the right to the protection of personal data since the law enforcement authority would have the possibility to obtain additional biographical data connected to the fingerprint. The right to data protection however may be interfered with, provided interference is done "in accordance with the law" and is "necessary in a democratic society to protect a legitimate public interest and the law is formulated with sufficient precision and is proportionate. As the proposed actions aim to combat terrorism and serious crime, they would clearly come under the umbrella of the exceptions. The proposed measure would have to ensure that any such interference would be proportionate, "in accordance with the law" and "necessary in a democratic society", and must comply with adequate safeguards such as purpose limitation and security of transmissions. It should be noted that even though the proposed measures would not oblige any collection of new personal data, since the data is already collected under the 'Eurodac' Regulation, it would imply a new processing activity for a different incompatible purpose to that for which they have been initially processed. The measures would only be regulating the access to such data. Although such measures should provide for adequate safeguards to mitigate the impact of the interference with the right to the protection of personal data, the fact that personal data will be used as such is already sufficient to be considered as a serious interference with the right to the protection of personal data according to the jurisprudence of the European Court of Human Rights

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Implementation costs for Member States' administrations	-√√	The following types of costs could be identified. First, the costs related to set up a secure communication channel to transmit the requests for consultation between authorities to consult 'Eurodac'. It is estimated that the costs related to the adjustment of the hardware in the Member States is in the range of 2,7 million EUR (27 x 100.000 EUR)[10]. Second, the costs related to the training of the staff authorised to consult 'Eurodac' and after a hit reply to consult the additional biographical data and the actual use of the staff. Member States have indicted in their replies to the questionnaire that specialised staff is necessary to perform a consultation of 'Eurodac' and that an additional one to two staff may be required. On this basis the costs are estimated on roughly 1,5 FTE. Based on an estimated hourly wage in EUR (average employment costs + 50% overheads) of 25 EUR and 1760 working hours per year (8 hours * 20 days * 11 months) the total yearly personnel costs for all MS would be 1.914.000 EUR for all Member States. Compared to policy option A, the costs related to an individual consultation would be lower because the consultation in policy option B would be based on the consultation of one database instead of the consultation of a law enforcement authority in another Member State on the basis of mutual legal assistance.

[10] The cost is estimated on the basis of the connection costs of the VIS system which is expected to be comparable.

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
EU budget	Sub-option (i)-√ Sub-option (ii)-√√	The costs related to set up a secure communication channel, a virtual private network to transport the data between the authorities concerned should be less than 1 million EUR. The costs related to the monitoring and evaluation of access to 'Eurodac' by law enforcement authorities are estimated at 500.000 EUR. Sub-option (ii) will generate additional costs at European level because the search functions of 'Eurodac' should be modified and the number of requests is likely to increase. The current system must also be adapted to allow searching 'Eurodac' with latents. This is not foreseen in the current contracts related to 'Eurodac'. The current project for a Biometric Matching System (BMS) contains a scenario for the integration of 'Eurodac'. The total costs for building and implementing the BMS will be divided over the three systems (SIS II, VIS, 'Eurodac') that it will serve. The share of the costs for the 'Eurodac' part cannot be exactly estimated but are around 2 million EUR, including a latent search capacity (with limited number of searches) and assuming that 'Eurodac' is hosted together with the BMS/VIS system. The total costs for the EU budget are estimated at around 2.5 million EUR for sub-option (ii) and 1.5 million EUR for sub-option (i).
Stakeholders views: Member States/law enforcement	√√	Member States expressed consensus that consultation should be allowed for the prevention, detection and investigation of terrorism and other serious crime. This option would contribute to enable this, since it would allow for the establishment of the identity of a victim of terrorism or of another serious crime offence who happens to be an asylum seeker or of a suspect of such a crime. Law enforcement stakeholders are of the opinion that access to 'Eurodac' is necessary to achieve an adequate level of efficiency in the prevention, detection and investigation of terrorism and other serious crime. The information contained in 'Eurodac' is required to establish the identity of a suspect or of a victim. This option would contribute to enable this, since it would allow for the establishment of the identity of a victim of terrorism or of another serious crime offence who happens to be an asylum seeker or of a suspect of such a crime.

Policy Option B: Access to 'Eurodac'		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Stakeholders views: civil society and data protection	-√√	Civil society representatives and data protection authorities expressed themselves against granting law enforcement access to Eurodac since such an access in their view would infringe the purpose limitation (asylum and immigration) and change 'Eurodac' into a criminal investigation tool. This option would grant law enforcement authorities the right to access Eurodac for the specific purpose of identifying the Member State that holds information on asylum seekers enabling the establishment of the identity of a victim of terrorism or of another serious crime offence who happens to be an asylum seeker or of a suspect of such a crime, hence would add another purpose to the initial purpose for which 'Eurodac' was established.

Policy Option C

Policy Option C: Access to 'Eurodac' and to additional biographical data		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Increasing security in the EU and facilitating the identification of victims by facilitating the verification of the identity of certain categories of third country nationals and closing the structural information gap	Sub-option (i)√√ Sub-option (ii)√√√	Same as Policy Option B. In addition, this option aims at regulating that the supplementary data should be made available in the case of a hit-reply from 'Eurodac', under a specific obligation in the proposed measure, instead of using existing instruments to gain access to such data. This would lead to further harmonisation at EU level of the national procedures following a hit in Eurodac, since that would be the best guarantee from a security angle that such additional information is always made available, including cases in which access to such information might have to be refused under existing instruments. The search possibility with latents will have a bigger impact since very often it is only possible to recover latents from a crime scene.

Policy Option C: Access to 'Eurodac' and to additional biographical data		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
Increasing security in the EU and facilitating the identification of victims by ensuring timely and less burdensome procedures for verification of the identity	√√√	Same as Policy Option B. However, instead of using existing instruments for the exchange of the additional data following a 'hit' in 'Eurodac', the Eurodac framework decision would explicitly regulate that the data should be swiftly made available under a specific obligation in the proposed measure, while using existing communication channels. This would guarantee that such additional information would be made available in a timely and non-burdensome manner, also in cases in which access to such information might have to be refused under existing instruments, which contain some exceptions.
Fundamental rights impacts		
Right to Asylum	-√	Same as Policy Option B. The interference with the right to asylum is effected by granting access to 'Eurodac'. The impact will not be greater if the proposed measures also govern the cooperation on additional information.
Protection of personal data	-√√√	Same as Policy Option B. The interference with the right to data protection is effected by granting access to 'Eurodac'. The impact will not be greater if the proposed measures also govern the cooperation on additional information. The same guarantees on data protection will exist for both Policy Options B and C.
Implementation costs for Member States' administrations	-√√√	Same as Policy Option B as regards the access to 'Eurodac' However, there would be additional costs for creating a new administrative and technical architecture for the exchange of the supplementary information. . The creation of a special procedure for the exchange of supplementary information will require an investment in each Member State for setting up this new procedure and training officers to use it. However, even though this matter was addressed in the questionnaire, Member States were not in a position to give an indication of possible costs.

Policy Option C: Access to 'Eurodac' and to additional biographical data		
Assessment Criteria	**Rating**	**Motivation of the rating and aspects of the policy option necessary to achieve the impact**
EU budget	Sub-option (i)-√ Sub-option (ii)-√√	Same as Policy Option B.
Stakeholders views: Member States/law enforcement	√√√	Same as Policy Option B. In addition, Member States law enforcement authorities were strongly in favour of making special provision for exchanging the supplementary information following a 'hit' in 'Eurodac'. This would facilitate the exchange of information between them and potentially by-pass the exceptions of the current instruments. It should be noted that the replies to the questionnaire were delivered by the Member States before the FWD 2006/960 becoming operational (i.e. before December 2008).
Stakeholders views: civil society and data protection	-√√√	Same as Policy Option B. In addition, civil society experts were not in favour of regulating access to supplementary information on the basis of the proposed measures. They considered that it would be sufficient if Member States used existing instruments to obtain such information.

COMPARING THE 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 costs of such an alternative will be considerable for Member States. In addition, the current situation where different access rights to asylum seekers data by law enforcement in Member States exist, will continue.

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 it assists on 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. These options also possess clear advantages in rendering the identification of victims of crime possible.

There is no similar centralised database containing data of EU citizens. As regards the possible discriminatory effect of consulting ‘Eurodac’ for law enforcement purposes in the light of Article 21 of the Charter, it must be noted that, in relation to the Visa Information System, which also contains data of only those third-country nationals which applied for a Schengen visa, similar mechanisms are in place. In addition, in most Member States access by law enforcement authorities to the national ‘Eurodac’ files is already possible. In none of these contexts has such access been considered discriminatory or illegal.

The negative impacts of Policy Options B and C could be reversed or at least reduced. The potential negative impact on the right to asylum could be reversed by adequate guarantees to guard against the possibility that law enforcement would divulge any information on the asylum seeker to his state of origin.

The impact on data protection could be reduced by appropriate adherence to the established data protection principles and guarantees. Access to 'Eurodac' should be permitted only for specific and limited purposes. Access should be limited to some designated authorities and only on a case-by-case basis, following a reasoned request and filtered by central access points that should be responsible for ensuring strict compliance with the conditions and procedures for access. The processing activity should be in full compliance with data protection principles and the rights of the data subjects. Accordingly, individuals should be given appropriate information and adequate rights of access, correction and redress (both administrative and judicial redress) and supervision by public independent authorities should be ensured.

Therefore between the "no action" policy and the legislative proposal policies, the legislative proposal policies present clear advantages. Access of law enforcement authorities to ‘Eurodac’ is the only timely, accurate, secure and cost-efficient way to identify whether and if so where data about asylum seekers are available in the Member States. No reasonable efficient alternative exists to ‘Eurodac’ to establish or verify the exact identity of an asylum

seeker that allows law enforcement authorities to obtain the same result. This unique identification is essential for law enforcement authorities in order to prevent and combat terrorism and serious crime involving third country nationals, as well as to protect victims of terrorism or serious crime. Access to 'Eurodac' cannot be considered disproportionate to the aims to be achieved. However, in order to avoid wrong identifications, it is important that the results of the comparison via 'Eurodac' are immediately checked by the Member State of origin that will be the only one responsible for making the final identification.

Between the two options involving legislative measures, both Policy Options present the same negative impacts on fundamental rights. Policy Option C would make supplementary information on the asylum seeker available between Member States through a special procedure where such is requested, while Policy Option B would use the existing instruments to facilitate access to such supplementary information. 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 higher 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. The exceptions and conditions on the exchange of data under FWD 2006/960, especially as regards coercively obtained data and data access which can be authorised only by a judge, are not such that would prevent the exchange of data where there is a legitimate reason to exchange the data. FWD 2006/960 has only been implemented as from December 2008 and until the time of drafting this report no problems on its functioning have been reported. In case that the functioning of this framework decision presents problems in the future, those can be addressed if and when they arise, taking into account additional costs.

In relation to the 2 sub-options regarding latents, even though the possibility to search 'Eurodac' on the basis of latents is more expensive, its contribution to the achievement of the objectives is fundamental and therefore would outweigh the impact on costs on the EU budget.

	Policy Option A	**Policy Option B**	**Policy Option C**
Increasing security in the EU and facilitating the identification of victims by facilitating the verification of the identity of certain categories of third country nationals and closing the structural information gap	0	Sub-option (i)√/√√ Sub-option (ii)√√/ √√√	Sub-option (i)√√ Sub-option (ii)√√√
Increasing security in the EU and facilitating the identification of victims by ensuring timely and less burdensome procedures for verification of the identity	0	√√	√√√

Fundamental rights impacts			
Right to Asylum	0	-√	-√
Protection of personal data	0	-√√√	-√√√
Implementation costs for Member States' administrations	0	-√√	-√√√
EU budget	0	Sub-option (i)-√ Sub-option (ii)-√√	Sub-option (i)-√ Sub-option (ii)-√√
Stakeholders views: Member State/law enforcement authorities	0	√√	√√√
Stakeholders views: civil society and data protection authorities	0	-√√	-√√√

THE PREFERRED POLICY OPTION

On the basis of the above, the adoption of legislative measures to ensure that law enforcement authorities have access to 'Eurodac' is the best policy option. It will ensure that the structural information and verification gap which exists in the EU as regards the exchange of asylum seekers data is closed, while ensuring that the access to such information can be provided in a straightforward and timely manner. At the same time, the preferred option does not go beyond what is necessary to achieve its objectives and only focuses on the essential aspects of the cooperation. Therefore the preferred policy option only focuses on providing the right for law enforcement authorities to request a comparison with 'Eurodac' data, while not regulating the ensuing exchange of supplementary information in case of successful comparison. 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 are currently in force instruments that regulate the exchange of law enforcement information between Member States, and there seems to be no reason to create special rules to regulate the exchange of information on asylum seekers. Access to asylum seekers' data by law enforcement should not be more favourable than access to any other data. Furthermore, there seems to be no reason for which a new costly organisational and technical architecture is established for the exchange of the supplementary information, when current systems are adequate and appropriate for this purpose.

Under Policy Option B, when a law enforcement authority is investigating a crime, it would have the following options: it could search its national databases on the basis of the fingerprint of its suspect. If it does not find information, it may try to search the national AFIS of other Member States using the Prüm Decision. If this is also unsuccessful, then it can search 'Eurodac'. If the 'Eurodac' consultation produces a hit, then the law enforcement authority could make a request to the Member State that introduced the information in 'Eurodac' under FWD 2006/960 in order to obtain supplementary information on the person to whom the fingerprint belongs. In the very rare cases where it cannot obtain the information using FWD 2006/960 (i.e. where the information is not available to the police with or without a judicial authorisation, or where the national law of the requested Member State would prohibit such an exchange of data), then the requesting Member State can try to obtain the information using mutual legal assistance.

The authorisation to search the fingerprint data contained in 'Eurodac' for the purposes of the prevention, detection and investigation of terrorism and other serious crime must be laid down in EU instruments. Because of the pillar structure of the EU, the authorisation for access and regulation of access to 'Eurodac' for law enforcement purposes would require two legal instruments. First, it would require an amendment of the 'Eurodac' Regulation in order to add a secondary purpose permitting the use of 'Eurodac' for law enforcement purposes by a "bridging clause". Second, it would require a new instrument under Title VI TEU that would regulate the modalities of such access by law enforcement authorities. Additionally, as the Title VI instrument would not apply to Iceland, Norway and Switzerland that are bound by the 'Eurodac' Regulation, these countries would have to give their consent to the amendment to that Regulation.

A proposal for an amendment to the 'Eurodac' Regulation in order to permit the use of 'Eurodac' for law enforcement purposes can only institutionally be presented by the Commission. Therefore, the objective of obtaining access to 'Eurodac' for law enforcement

purposes can only be achieved by EU action. As a result, the Commission is better placed to also present the accompanying proposal for a Council decision under Title VI TEU regulating the actual access and use of the data held in 'Eurodac' by law enforcement authorities.

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 option 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 opinion 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. The reference to a definition of serious crime as already used in an existing instrument, i.e. the European Arrest Warrant Framework Decision presents many advantages from a legal certainty point of view. The reason is that, as Member States co-operate in a variety of areas and exchange various different types of information, it is very important that there is certainty and consistency on which areas they can in fact cooperate. In addition, this definition is one that has been agreed by Member States and which has been a point of reference in other instruments on police co-operation. However, it is understandable that asylum seekers should not be penalised for crimes that might have been committed in their effort to flee from the state of origin, for example entering illegally in the territory of the Member State where they seek protection. Sub-option (iii) would be a compromise between the other two sub-options, whereby legal certainty is maintained, while taking into consideration the special requirements of 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. In view of the huge differences in the way in which Member States have organised their law enforcement authorities in terms of competences and organisation, sub-option (ii) would require tremendous efforts in terms of comparing the different law enforcement agencies of the Member States, whereas the issues for which access to Eurodac is being sought are not directly related to the manner in which Member States have organised their law enforcement agencies. Hence such an approach would not present any added value in terms of the issues for which access to Eurodac is being sought compared to sub-option (i) in which it would be left to the Member States to determine the competent authorities.

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 and, if so, the duration of that limit.

(i) A sunset clause could be introduced in the bridging clause in the Regulation. Such a clause would be a provision repealing the bridging clause at a specified time period, unless its application is *expressis verbis* extended by the Council, based on an evaluation report drawn

up by the Commission. To facilitate this process, and hence a possible extension of the application of the bridging clause, specific and well-defined indicators can be included in the sunset clause. The sunset clause can be triggered independent from the fact whether the structural information and verification gap continues to exist or not.

(ii) The sunset clause would repel the Regulation only in case that it has been established on the basis of the Commission evaluation that the measure has not proven to be effective and necessary.

(iii) A regular evaluation mechanism can be foreseen without a sunset clause in the Regulation, also including specific and well-defined indicators. In this scenario no time limit would apply. However the evaluation could recommend changing or abandoning the instrument..

To sum up, depending on the policy sub-option chosen:

- the instrument would not be applied after a certain time unless the Council, after the evaluation by the Commission, decides otherwise

- the instrument would not apply after a certain time unless the evaluation by the Commission proves it is necessary

- the instrument would continue to apply unless the evaluation of the Commission proves that it should be amended or abandoned.

The various consultations that have been undertaken for the purpose of preparing this impact assessment, including the replies of the Member States to the questionnaire, have shown that an option of access to 'Eurodac' should have the following parameters:

– Each individual request for consultation should be duly reasoned, which means that it should justify why in a specific case access is legitimate, necessary, appropriate, adequate and proportional;

– The database could only be consulted on a case-by-case basis. Access on the basis of mass comparisons would be explicitly prohibited.

– Public independent authorities would carry out oversight.

– Onward transmission to any third country should be strictly prohibited.

– There should be special provisions on data security.

– There should be specific provisions to ensure compliance of processing activities with data protection principles and the rights of the data subjects.

– In view of the role of Europol in the fight against cross-border organised crime, in particular by providing the necessary coordination tools to national law enforcement authorities, it should have the same access rights as the designated law enforcement authorities of the Member States.

MONITORING AND EVALUATION

It is important that the consultation of 'Eurodac' would be subject to monitoring and evaluation. Such arrangements could be:

An in-depth evaluation of the effectiveness of consulting 'Eurodac', containing information on the exact purpose of the access for consultation, the volume of consultations, the number of cases which have ended in successful identifications and verifications and the number of cases on which access was denied and the reasons for the denial, and report on number of cases on redress related to data protection and their outcome. Member States and Europol should communicate such reports to the Commission. The evaluation provisions in the Regulation would include a sunset clause, depending on the sub-option which is finally chosen.

The Commission could review the operation of the access to Eurodac the latest within three years from its entry into force and submit a report to the Council. This should monitor whether access to 'Eurodac' has met its objectives and whether Member States have complied with their obligations. The review should also examine whether the system has been successful and justify its conclusions with statistics. The review should also take into account the annual reports of the Member States and Europol and consider all matters arising there from.

Depending on the sub-option chosen, the evaluation could result in:

- providing a basis for a possible decision to trigger the sunset clause

- application of the sunset clause if the evaluation of the Commission proves that the instrument is not necessary

- leaving the instrument in place/ proposing amendments/ withdrawing it depending on the findings of the evaluation.

Annex 1:

COMPILATION OF THE REPLIES TO THE QUESTIONNAIRES OF THE 27 EU MEMBER STATES, ICELAND, NORWAY AND SWITZERLAND AS WELL SENT TO EUROPOL

INITIAL QUESTIONNAIRE

The Commission received 25 replies to the questionnaire.

PART I: ACCESS AND CONSULTATION TO THE 'EURODAC' SYSTEM

For which purpose(s) in relation to terrorist offences and other serious criminal offences, should police and other law enforcement authorities be allowed to consult the 'Eurodac' system?

The consensus was that consultation should be allowed for the prevention, detection: and investigation of terrorism and other serious crime.

More and more law enforcement authorities are confronted with the problem of individuals travelling without identification papers or falsified papers that refuse to give out who they are or assist the police in finding out who they are. The information in 'Eurodac' could be in some circumstances the only available information to identify a person. Access for law enforcement authorities to 'Eurodac' could help to establish the identity of the person. One argument brought up in favour of allowing access to consult 'Eurodac' for the three purposes mentioned above was that that **timely detection** and investigation of criminal offences can be instrumental to prevent other crimes, including terrorist offences.

Most respondents suggested allowing searches for the offences referred to in Article 2 (2) of the European Arrest Warrant Framework Decision. One respondent referred to the definition applied in the VIS Council Decision.

One respondent suggested to allow searches to establish whether asylum applicants **abuse the European asylum system** to elude justice, as perpetration of certain serious crimes would jeopardise the right to obtain asylum; in that respect both migration authorities and police authorities should have the possibility to exchange knowledge about a person to maintain and protect public order, which is an aim of the Geneva Convention, with due respect however of fundamental rights obligations incumbent on Member States; respondent concerned observed that the current strict separation between asylum processes and the domain of the maintenance of public order presents a risk.

Europol replied that its access should be based on Article 2 of the Europol Convention. A respondent considered the concept "detection" unclear.

Referring to Article 5 and 8 of the 'Eurodac' Regulation, which one of the data contained in the 'Eurodac' system, should be made available in case of a hit?

The vast majority of respondents noted that all the data of Articles 5 and 8 should be made available in case of a hit. It is especially important to receive the fingerprints from 'Eurodac' because of the need to compare to crime scenes and identify suspects at the earliest

opportunity. The Member State making the enquiry may only possess latents and requires a set of fingerprints for comparison purposes, the Member State making the enquiry may not possess a full set of fingerprints and may wish to conduct further fingerprint searches which relate to the original enquiry and therefore access to the 'Eurodac' set may be helpful, the Member State making the enquiry may not possess a good quality set of fingerprints and may wish to conduct further fingerprint searches which relate to the original enquiry and therefore access to the 'Eurodac' set may be helpful.

Should consultation of the 'Eurodac' system by police and other law enforcement authorities be allowed on the basis of ten fingerprints only or also on the basis of latents?

23 respondents thought that consultation of the 'Eurodac' system by police and other law enforcement authorities should be allowed on the basis of ten prints and also on the basis of latents. However, access to 'Eurodac', even only on the basis of ten finger prints would be of great use for police, even if it was not possible to include the check of latents.

It was that latents help to detect the perpetrator of an unsolved crime and to contribute to accurate identification. One respondent clarified that comparison of latents to immigration databases demonstrated a significant hit rate. Some respondents stated that the consultation of latents should only be permitted as a last resort, i.e. if the identity of a perpetrator can not be established in any other way. Two respondents were of the opinion that the different technical possibilities of the 'Eurodac' system should be looked into first.

In case data of persons apprehended when illegally staying on the EU territory would be stored in 'Eurodac', should those data be accessible for consultation by police and other law enforcement authorities? Please state the reasons for your answer.

All replies were affirmative. The fingerprint data of persons apprehended when illegally staying on the EU territory (CAT3) may be useful for police investigations in the same way as fingerprint data as for CATs 1 and 2. Moreover, the fact, for example, that a person was apprehended in different Member States may be of particular importance to reveal cross border crime.

Referring to the data listed under question 2 (above), should other search criteria than fingerprints be allowed?

Eight respondents replied affirmatively, while thirteen respondents replied negatively. Two of those which replied affirmative suggested additional search criteria, including photographs, name and date of birth.

Please indicate which authorities in your country should be allowed to consult the 'Eurodac' system. Please state the reasons for your answer.

The authorities which were mentioned are central investigation services with fingerprint experts, the same categories of authorities that have access to CATs 2 and 3 data of the 'Eurodac' Regulation, security and intelligence services, immigration and nationality services, the department of the Public Prosecutor and authorities subordinate it, police and other law enforcement authorities, border guard authorities and fire brigades. One reply suggested regulating the issue of the nature of authorities on the basis of the VIS Council Decision.

How should the 'Eurodac' system be consulted by police and possibly by other law enforcement authorities? Please state the reasons for your answer.

The majority of respondents (16) believed that consultations should take place via a single national central access point, while others (5) believed that there should be direct access. 6 respondents believed that consultation should take place via more than one national central access point. One respondent referred to the existing national contact points for 'Eurodac'. A respondent was of the opinion that the number of access points should be left to the discretionary power of the Member States. The replies reflected that the concept of a national access point was not understood as the national existing access points to 'Eurodac' but was as new access points, front offices to the national access points of 'Eurodac'.

What do you consider to be the appropriate time frame within which an answer to the request for consultation of the 'Eurodac' system should be available to the police or other law enforcement authority that is at the origin of the consultation? Please state the reasons for your answer.

The replies varied. The respondents noted as the appropriate time frame: as soon as possible, within one hour, within 24 hours, within 24 hours for exceptional cases of urgency and within 72 hours for ordinary cases, not more than 5 days. Other respondents noted that the timeframes should be the same as for the 'Eurodac' Regulation or the Prüm Decision or the FWD 2006/960.

It was stressed that there is a difference between consulting 'Eurodac' on the basis of ten fingerprints and latents, which would require more response time. Further, it would be unrealistic to provide results for law enforcement in less time than they are provided for Dublin users. To do so could affect the service to current users.

For which occasion or occurrence should consultation of the 'Eurodac' system be allowed? Please state the reasons for your answer.

in a specific case : 11

in every case related to the prevention, detection or investigation of a terrorist offence or of another serious criminal offence : 15

on the basis of mass comparison, for instance comparing a certain number of unsolved latents (UL) or Fingerprints (TP) related to terrorist offences or serious criminal offences to fingerprints (TP) stored in the 'Eurodac' system : 10

on a case-by-case basis & Prüm did not lead to results : 1

Some respondents referred to the system applied in the **VIS Council Decision** that is based on access only in a specific case. Those respondents, which were in favour of access in every case explained at the expert meeting that the ticking of the criminal offence, as listed in Article 2 (2) would be sufficiently specific. One of the respondents supporting mass comparison referred to comparing a certain number of unsolved latents or fingerprints related to terrorist offences or serious criminal offences to fingerprints stored in the 'Eurodac' system.

In case you marked "in a specific case" in your reply to question 9, which aspects should be examined prior to allowing consultation of the 'Eurodac' system? Please state the reasons for your answer.

The replies referred to the seriousness of the specific terrorist offence or other serious criminal offence, the necessity to consult the 'Eurodac' system, the proportionality of the request, when the consultation will substantially contribute to the prevention, detection or investigation of the offence, and prior consultation of the national AFIS via Prüm channel.

Several respondents considered all aspects relevant. One respondent supported the model applied in the VIS Council Decision. At the expert meeting some experts considered the examination no comparable to the examination provided in the VIS Council Decision, since the only possible output by 'Eurodac' is a hit-reply.

In which form should consultation to the 'Eurodac' system be allowed? Please state the reasons for your answer.

The respondents believed that consultation should be allowed on the basis of a reasoned written request (5 replies), on the basis of a reasoned electronic request (13 replies), on the basis of a written request (1 reply), or on the basis of a electronic request (11 replies).

A **reasoned written request** could be used in exceptional circumstances, like technical problems that prevent the electronic transmission of a request.

The majority of respondents identified consultation on the basis of a reasoned electronic request because it is the speediest, it is the easiest to implement, it would prevent unauthorised access and it would provide an audit trail.

Several respondents preferred an **electronic request** because the hit/no hit answer of 'Eurodac' does not demand prior justification of the request, while a check on the reason underlying the request should be checked at the level of the end-user.

One respondent clarified that the access should be as it its, through one national contact point without independent control authority. The personnel working on the 'Eurodac' system should, just like the staff of for instance the Interpol office or SIRENE, check if the requirements are met before consulting 'Eurodac'. Consultations should be logged. If access is facilitated through a single national contact point, the office responsible for transmitting fingerprints through 'Eurodac' would verify that the conditions for transmission are met and then send the fingerprints (or latents) through 'Eurodac' on basis of electronic request.

Several respondents stated that only a <u>further</u> request after the hit-reply should be subject to a reasoned written request.

Should the consultation procedure (questions 7, 8, 9, and 10) differ depending on the urgency of the case? Please state the reasons for your answer.

11 respondents thought that the procedure should be different in case of urgency, while 12 did not think so. One of the arguments raised against a different consultation procedure in the case of urgency was that the system would become too complicated. One respondent thought the request should be processed by the requested authority on the basis of Interpol standards, i.e. in exceptional cases of urgency as soon as possible, at least within twelve hours.

PART II: ACCESS TO FURTHER PERSONAL DATA

Should access to further personal data linked to the data recorded in the 'Eurodac' system, such as name, place and date of birth of the data subject, be covered by the legislative proposal? Please state the reasons for your answer. Alternatively, specify the legal instrument by which means such further personal data should be obtained (for instance Framework Decision 2006/960/JHA, Mutual Legal Assistance, sui generis instrument to be created, other).

14 replies suggested that further data to be covered and 6 that they should not be covered. The respondents against the regulation of further access within the framework of the proposed legislation thought that the existing legislation is sufficient for police and other law enforcement authorities to get access to further personal data.

The respondents which replied that the further data should be covered by the proposal suggested that access to such data could be achieved by: a sui generis legal instrument, the establishment of a DubliNet-like network, access on the basis of FWD 2006/960/JHA, additional first pillar legislation, access via Mutual legal assistance, regulation in the 'Eurodac' Regulation and 'Eurodac' Decision

If the answer to the previous question is that access to further personal data should be covered by the legislative proposal, or that a sui generis instrument should be created:

Which further personal data should be covered?

The following data categories were identified: all personal data held in 'Eurodac', data gathered along with the fingerprinting, including the time and reason for fingerprints, the country which fingerprinted and the reference number, the name and surname (at birth and later surnames) of the data subject, earlier names, alias, the place, country and date of birth, the particulars of used documents, including the identity card or passport (number, period of validity, date of issue, issuing authority, place of issue, etc.), present and / or previous nationality, first names of parents, a description of the person's characteristics, e.g. height, colour of hair and eyes, known arrest and whereabouts search requests, place of residence, known whereabouts and routes travelled, previous criminal offences, expulsion or deportation from EU states, sex, all other personal data useful for detection or investigation, and the data categories identified in Article 21 (2) of Regulation (EC) 343/2003.

Within which timeframe should further personal data be obtained?

The current accepted timeframe in the Dublin system (up to two months) was considered as absolutely unworkable for law enforcement purposes. Replies referred to response times provided for in Framework Decision 2006/960/JHA and the Interpol response time. Other replies referred to timeframes of immediately, one hour, 24 hours and one or two weeks.

How should this access take place (for instance direct contact between authorities entitled to consult the 'Eurodac' system, via contact point(s), other)?

Europol thought this should be organised via the Europol National Units. Other respondents indicated via a national point of contact or by direct contact between the law enforcement authorities or between the authorised users of the 'Eurodac' system. One respondent was in

favour of inserting those personal data in the NIST file, so that the data could be forwarded in the hit message.

Which communication channels should be used for the exchange of information?

The replies indicated that communication could take place via electronic channels, the Interpol channel, direct contact between the authorities competent to consult 'Eurodac', or via the DubliNET.

Under which conditions should this access take place?

In one reply it was stated that this should be organised on the basis of an existing national legal base and existing or further bilateral or multilateral international agreements. Regarding storage in the NIST file (standard encoding of fingerprints), access should be able as an attachment to the ancillary data delivered next to the hit reply or via a national access point and the law enforcement authorities, directly between the authorities which are entitled to consult the 'Eurodac' system.

Access should be subject principles of proportionality, data safety and security and via the national access points. One respondent replied that as a rule the migration authorities should be informed on any request in the case of a hit-reply. One respondent thought that persons entitled to access 'Eurodac' should have a written authorisation.

For how much time should data obtained under the legislative proposal be retained?

12 replies suggested that the data should be retained for a fixed period of time, while 9 indicated that the data should be retained for a period to be determined by the national law of the requesting Country. Two respondents thought that data should be retained for as long as it is being used for law enforcement purposes. Another respondent clarified that national law should apply.

Should there be an obligation for the Central Unit of 'Eurodac' to notify the competent authority that consulted the 'Eurodac' system on the basis of the legislative proposal that the further personal data regarding the data subject have been blocked or erased in 'Eurodac'?

11 respondents replies affirmatively while 9 replied negatively. Among the arguments in support of a negative response, it was stated that the Central Unit has no power in relation to the additional biographical data. One respondent thought that the existing 'Eurodac' rules in this respect should remain unchanged.

Generally, it would be difficult to accept that 'Eurodac' would be able to block the passing of personal data or that data has been erased unless stipulated by Member State of origin.

PART III DATA SECURITY AND DATA PROTECTION

Which data security rules should apply to the consultation of the 'Eurodac' system? Please state the reasons for your answer

Most replies supported the existing data security requirements applicable to 'Eurodac'. A minority of respondents referred to the Framework Decision on Data Protection. One

respondent favoured a strong audit trail to be applied to periodically monitor the requests to the consultation of the 'Eurodac' system. Europol stated that the data security requirements in the Europol Convention will be applicable.

Which data protection rules should apply to the consultation of the 'Eurodac' system? Should the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters apply? Please state the reasons for your answer.

Several respondents supported the application of the **Framework Decision on Data Protection**. Europol made clear that the Framework Decision on Data Protection will not be applicable but the data protection requirements in the Europol Convention will be applicable.

One respondent was of the opinion that the processing of personal data retrieved under a future 'Eurodac' Council Decision should be subject to a data protection level in its national law which at least corresponds to that resulting from the **Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data** and the **Additional Protocol** of 8 November 2001 to that Convention, and shall take into account **Recommendation No R (87) 15 of 17 September 1987** of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector.

Another respondent expressed itself against onward processing of 'Eurodac' data to **third countries** or international organisations and against any contact with the country of origin, to prevent frustration on the asylum procedure and to prevent that the country of origin of the asylum seeker will find out the request for asylum. Another considered transfer of 'Eurodac' data to a third country acceptable on the basis of an adequacy finding.

In one reply the respondent made a distinction between a query in 'Eurodac' that only leads to hit / no-hit-reply and a request to further personal data, requiring a reasoned request.

How should the supervision of the* consultation *of the 'Eurodac' system be organised and - where relevant - of the processing of the* further personal data*? Please state reasons for your answer and make a distinction between ex-ante control and ex post control.

The replies suggested that ex-ante control could be carried out by an internal check on a request to consult the 'Eurodac' system, while only one respondent thought that there should be an independent internal check on a request to consult the 'Eurodac' system. It was considered that the internal check was justified by the considered moderate impact on data protection of the data subject. A hit-reply does not reveal any identification. Only access to further personal data would justify a more intense ex-ante control.

According to the respondents, ex post control should be carried out by national Data Protection Authorities. Ex post verification and auditing in conjunction with data logging of data processing operations by the national data protection authorities was only preferred by two respondents. According to a respondent there must be an independent check carried out on all law enforcement requests to ensure that the system is not abused. Reasoned written /electronic requests for each search will assist in ensuring that access to 'Eurodac' is not abused.

SUPPLEMENTARY QUESTIONNAIRE

The Commission received 13 replies to the questionnaire.

A. The number of actual consultations on asylum seekers' fingerprints

How many consultations of your national data filing system containing the fingerprints from asylum seekers do law enforcement authorities carry out each year for the purposes of prevention, detection and investigation of terrorist and other serious criminal offences? This refers both to direct consultations as well as the consultations via contact point or the third party of asylum seekers.

The law enforcement authorities of all 13 Member States had direct or indirect access to fingerprints of asylum seekers. While three Member States keep the fingerprints of asylum seekers in the same database as those of other third country nationals, six Member States and two Dublin States keep them in their general fingerprints database (AFIS). The majority of Member States do not keep statistics and were unable to provide further data.

How many requests do your law enforcement authorities issue per year to consult the data filing system mentioned under question 1 of other Member States for the purposes mentioned? In how many cases per year is a single request issued to several Member States because no information is available about the Member States that could have processed an asylum request?Only four Member States were able to provide such statistics. One Member State mentioned approximately 5000 requests while another around 60.

Provided such data is available: In how many cases of the situations covered by questions 1 and 2 has the consultation of data filing systems containing fingerprints of asylum seekers were helpful in the prevention, detection or investigation (prosecution) of terrorist offences and other serious offences? If no such data is available, please provide some (real life) examples.

The majority of Member States were unable to provide such statistics. One Member States mentioned 850 hits on criminals. Member States that keep fingerprints of asylum seekers with other fingerprints, mentioned a 7% hit rate, 10% hit rate, and 9000 yearly hits.

How many times per year are the responsible authorities of your country recipient of a request mentioned under question 2 issued by another Member State?

The majority of Member States do not keep statistics. Some Member States mentioned statistics relating to mixed fingerprint queries, including 3529 requests, 3763, 3000 and 6292 requests.

In general, have there been cases or incidents in which the consultation of your national data filing systems containing fingerprints from asylum seekers have been considered unlawful? If yes, please specify.

Member States reported that there have been no such instances.

What control mechanisms are in place to prevent the misuse/abuse of the possibility for law enforcement purposes to consult national data filing systems containing fingerprints from asylum seekers?

Several control mechanisms were mentioned, including a reasoned request for access, consultations done through a single point of access that checks all requests, auditing, checks by the data protection authorities, and other guarantees under national law.

Based on the current number of the requests (question 2 above), do you expect that the number of requests would change if 'Eurodac' can be consulted? Would the number of the requests increase, e.g. because of the consultations will become less burdensome, or decrease, e.g. because 'Eurodac' will increase efficiencies by indicating whether and if so: in which Member States further personal data about the asylum seeker can be obtained. Please provide an estimation of future number of consultations.

The majority of Member States expected the number of requests to decrease, while consultation of 'Eurodac' to increase.

B. Financial part

Referring to question 1 of section A, what are the relative and/or absolute cost elements of a consultation of national database on the basis of a national request in particular manpower (number of staff involved) and infrastructure? How many working hours are involved in average in processing a consultation and costs per hour?

The questions varied from 15 minutes to one day, but all agreed that specialised staff is required to perform the consultation.

Referring to question 2 of section A, what are the relative and/or absolute cost elements of a consultation of national database on the basis of an ongoing request in particular manpower (number of staff involved) and infrastructure? How many working hours are involved in average in processing a consultation and costs per hour?

Referring to question 2 of section A, what are the relative and/or absolute cost elements of a consultation of national database on the basis of an incoming request in particular manpower (number of staff involved) and infrastructure? How many working hours are involved in average in processing a consultation and costs per hour?

The questions varied from 15 minutes to 2 hours.

'Eurodac' could only provide a 'hit reply', which means that law enforcement authorities should obtain additional data related to the matching fingerprints to take law enforcement action. What are the relative and/or absolute cost elements of the processing of an incoming request to provide additional data in particular manpower (number of staff involved) and infrastructure? How many working hours are involved in average in processing a consultation and costs per hour?

The replies varied from 30 minutes to 8 hours.

How would the access to 'Eurodac' change the costs referred to in questions no. 1, 2 and 3 of this section? What type of savings (e.g. increased efficiency) or additional expenditure (establishing access points for 'Eurodac')?

The Member States generally find it difficult to estimate because they cannot predict the number of hits and the number of requests for supplementary information. The majority of

Member States do not believe that they would require additional staff and investment in case that access to 'Eurodac' is permitted, while other believe that an additional 1-2 trained staff might be required.

C. Types of criminal offences

Referring to your replies to the question under section A, please indicate the crimes for which your national law allows consultation of the national (fingerprint) data of asylum seekers for the purpose of prevention, detection and investigation.

The majority of Member States have access to asylum seekers fingerprints for all the prevention, detection and investigation of all crimes, while some Member States limit such access to crimes that are punishable with imprisonment.

Does your national law also consultation to prevent, detect or investigate inciting, aiding, abetting and attempting of the criminal offences referred to in your reply to the question 1 of this section?

All Member States permit such consultations.

Annex 2

OBSERVATIONS MADE BY THE EXPERTS

For the purpose of the preparation of this Impact Assessment report, the Commission services consulted the following stakeholders:

Law enforcement stakeholders of the Member States, Iceland, Norway and Switzerland as well as Europol on 25 and 26 September 2007

Stakeholders representing civil society on 8 October 2007

Representatives of the national data protection authorities of the Member States, and of Iceland, Norway and Switzerland as well of the Joint Supervisory Body of Europol and of the European Data Protection Supervisor on 11 October 2007.

1. The purposes for consultation of 'Eurodac'

Law enforcement stakeholders confirm that access to 'Eurodac' by the enforcement is necessary to achieve an adequate level of efficiency in the prevention, detection and investigation of terrorism and other serious crime. In their view, the information contained in 'Eurodac' is required for two reasons: to identify a person suspected of committing or having committed such offence or of a victim thereof, and to verify the identity of a suspect or a victim if there are serious doubts about his identity. Access to 'Eurodac' should only be permitted if there are well founded grounds to believe that consultation can assist the identification or verification.

Law enforcement authorities pointed out that the obligation of asylum applicant to provide fingerprints is a feature of the Dublin system and is considered necessary and proportionate, and does not jeopardise the right to asylum. Access to such data by law enforcement authorities for the purpose of prevention and fight against crime is also necessary and proportionate and will not interfere with the right to asylum.

The legislation providing law enforcement authorities with access to the VIS[11] shows that access of law enforcement to a non-law enforcement information system is possible. It shows that it is possible to strike a fair balance between security needs and data protection safeguards by imposing conditions incumbent on the law enforcement users of the first pillar information system. However, civil society argues that the position of 'Eurodac' is not comparable to the position in VIS. The position of an asylum seeker would be very different from that of a third-country national tourist, who would always have the choice to decide

[11] The Visa Information System is a system that contains personal data related to visa applicants by third country nationals. The Council Decision regulates the access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. An applicant for a short stay visa who happens to have the nationality of a third State subject to a visa obligation is obliged - in the same way as an asylum applicant, to provide fingerprint data as well as other personal data to the visa issuing authority. If this person does not respect the visa obligations and is subsequently apprehended when illegally crossing the border or is illegally residing on the territory of the EU, (s) he can be coerced to provide fingerprints to allow checks against the 'Eurodac' system.

whether or not to apply for a visa taking on board that law enforcement authorities may in the future access the VIS under certain conditions.

Experts representing civil society are afraid that potential asylum seekers will be discouraged from requesting asylum if access to 'Eurodac' is allowed for law enforcement purposes. It would be exacerbated by the fear that access by police and other law enforcement authorities in the Member States and by Europol to information about the asylum seeker could end up in the hands of authorities of their country of origin. If such would happen, it could expose relatives or friends of the applicant, or the applicant him or herself to the risk of inhuman treatment. Law enforcement stakeholders agree that legislation should provide for guarantees to prevent misuse of personal data on the asylum seekers. Strict rules regarding data security and the transmission channels should be enshrined in law.

Data protection authorities and representatives of civil society consider that the further use of 'Eurodac' is unacceptable because such access would infringe the purpose limitation principle and change 'Eurodac' into a criminal investigation tool. This would be contrary to the specific purpose of 'Eurodac' that is based on an asylum and immigration legal basis of the EC Treaty.

Civil society experts believe that it is discriminatory that asylum seekers fingerprints are taken and accessible to law enforcement authorities and fingerprints of normal citizens not. One expert considered that therefore the fingerprints should be taken of all citizens. Asylum seekers will have a bigger chance to be subject to law enforcement thanks to fingerprint identification compared to normal citizens. They were of the opinion that it will therefore stigmatise asylum seekers.

2. The necessity of consultation of 'Eurodac'

The experts presented examples and scenarios supporting the need to access 'Eurodac' to tackle crime could otherwise not be solved or only in an inefficient manner. They highlighted that 'Eurodac' contains information that is not readily available from other sources or through other information channels. The need for access was corroborated by the following observations.

Efficient law enforcement requires that suspects are uniquely identified as soon as possible and that alleged identities are verified. Only fingerprint-based information makes this possible.

Fingerprint comparison via 'Eurodac' maybe the only manner to uniquely identify a third country national about who no reliable, stable or coherent biographical information is available. In some cases 'Eurodac' is the only information available about an individual who is no resident of or does not have the nationality of one of the signatory states of the Dublin Regulation. Further, in most cases it is the only fingerprint information available about third country nationals.

Access to data recorded in 'Eurodac' avoids that a law enforcement authority has to request access to personal national asylum data from each Member State individually. The identification of the Member State that entered the fingerprint data into 'Eurodac' will save considerable time to obtain the further biographical data of the asylum seeker that that Member States recorded.

Rapid resolution of identities through 'Eurodac' allows saving considerable time and manpower whilst achieving higher levels of law enforcement. Timely detection and investigation can lead to successful prevention of terrorist offences or other serious crimes.

Data protection authorities considered access to 'Eurodac' not only unnecessary but also disproportional and against the principle of fairness. Some experts were of the opinion that , if access to 'Eurodac' under conditions should be allowed after all, every Member State should separately demonstrate that it is legally and practically prepared to manage access 'Eurodac' for law enforcement purposes. This could be organised by peer evaluations.

3. The scope

Access to fingerprint data contained in 'Eurodac' might often be necessary to assist law enforcement authorities in their task to prevent, detect and investigate criminal offences. 'Eurodac' is searched with fingerprints only and returns, in case the reference set matches a recorded set of ten fingerprints, a hit-reply confirming the match, as well as some additional data, including the reference number that links the fingerprint data with a record held in a separate national database in the Member State that recorded the fingerprint data in 'Eurodac'. The separate file contains further biographical data of the asylum applicant. Law enforcement stakeholders insist that access to data recorded in 'Eurodac' is more efficient unless the further biographical data of the asylum applicant are not readily accessible. These additional data should be swiftly made available in the case of a hit-reply from 'Eurodac'.

Some experts of civil society are of the opinion that the Council conclusions of 12-13 June 2007 should be interpreted as inviting the Commission only to prepare legislation to regulate access to the data recorded in 'Eurodac'. They also object to access by Europol to 'Eurodac' because it is not comparable to the law enforcement authorities of the Member States. Some data protection stakeholders share that view.

4. The types of crime for which access is justified

Law enforcement stakeholders are of the opinion that the prevention of and fight against the criminal offences listed in Article 2 (2) of Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant[12] (EAW Framework Decision) justify access to consult 'Eurodac' data.

Civil society stakeholders and data protection authorities are of the opinion that the scope of the crimes listed in Article 2 (2) of the EAW Framework Decision is too wide and should be restricted to specific extremely serious offences. Some experts stated that access for reasons of crime prevention should be treated differently from consulting 'Eurodac' for investigation. The concept of prevention would be too vague and lead to using 'Eurodac' for unrelated purposes, i.e. allowing fishing expeditions. The range of crimes allowing access to consult 'Eurodac' for crime prevention should be restricted, for instance only to terrorist offences, and only in case of a concrete and imminent danger of a terrorist attack which would cause great bodily harm and if the risk is based on concrete facts.

[12] OJ L 190, 18.07.2002, p.1.

Law enforcement stakeholders recognize the data protection, but were of the opinion that these could be catered for by providing for access on a reasoned case-by-case basis related to a specific criminal offence in an agreed list of offences.

5. The types of data recorded in 'Eurodac' to be consulted other than fingerprints

Law enforcement stakeholders stated that it is vital that they receive with each hit in 'Eurodac', the reference number of the fingerprint record allocated by the Member State of origin as well as the indication of that Member State. Furthermore when necessary and proportional, a law enforcement authority may request, in case of a hit, access to the other data recorded in 'Eurodac' in conjunction with the fingerprint.

6. The access to additional supplementary information

The categories of supplementary information that each Member State records in addition to the fingerprint data in 'Eurodac' are laid down in Article 21(2) of Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (the Dublin II Regulation). Law enforcement authorities stated that access to these data is in general appropriate, relevant and non-excessive, as well as necessary to take law enforcement action. As was set out above, access to the fingerprint data without the possibility to promptly consult the additional biographical data related to the person whose fingerprints are recorded would not be efficient from a law enforcement perspective.

For example, when consultation of 'Eurodac' informs the police authorities of a Member State that the fingerprint data of a person arrested on the suspicion of having committed a serious crime are stored in 'Eurodac', 'Eurodac' always provides the fingerprint print data, the gender of the person involved, the date on which the fingerprints were taken, the date on which the data were transmitted to the Central Unit of 'Eurodac' and the reference number used by the Member State of origin and the identity of that Member State. Police authorities must know the name of the person involved as well as other biographical data to prosecute the arrested person.

Two EU legal instruments could be used to obtain those biographical data. Framework Decision 2006/960 if the police in the requested Member State has access to the data, and the national law of that State does not consider that these data were obtained by means of coercive measures. If that instrument cannot be used, Member States can use mutual legal assistance. This situation leads to different possibilities to obtain data across the EU and does not create a level playing field for law enforcement authorities. Member States have very different ways to manage additional biographical data: in some police collects, stores and accesses these data, whereas in other they are in the remit of immigration authorities.

A majority of law enforcement stakeholders that addressed the issue hold that the legislative proposal providing for access to 'Eurodac' should also contain rules and procedures to access further biographical data. Civil society stakeholders considered that any possible future legislation should be restricted to regulating access to 'Eurodac'. It is sufficient that the requesting law enforcement authority know in which direction he should go to obtain additional data.

7. The categories of authorities authorised to access 'Eurodac' for law enforcement purposes

All law enforcement stakeholders hold that police and other law enforcement authorities such as customs should have access. Some stated that access should also be granted to border control authorities and immigration authorities for law enforcement purposes.

A minority maintained that intelligence and security services should be entitled to access 'Eurodac'. National data protection authorities and civil society stakeholders however oppose such access. The Commission observed that Article 33 TEU and 64(1) TEC exclude national security and the maintenance of public order from the scope of competence of the European Union. It can therefore not be substance of EU legislation.

8. The conditions and modalities for searching and accessing 'Eurodac' in normal circumstances as well as in exceptional cases of urgency

This Impact Assessment identifies different situations under which 'Eurodac' can be consulted. In an exceptional case of urgency conditions for consultation may have to be adjusted to save time.

8.1. The conditions for searching and accessing 'Eurodac' in normal circumstances

Law enforcement stakeholders consider the seriousness of an offence as the most relevant condition justifying access to 'Eurodac'. Moreover they stated that first the national AFIS should be consulted, and subsequently the fingerprint data available on the basis of the proposal for the Prüm Decision. Consulting 'Eurodac' by law enforcement authorities is conceived as a means to identify or to verify the identity of a person after other means of identification have failed or have proven not to be appropriate.

Stakeholders are divided as to whether access should be on a case-by-case basis only or should also be allowed in general for each case related to a crime listed in Article 2(2) of the EAW Framework Decision. Consultation on a case-by-case basis demands to reason each request whereas in the latter case it would be sufficient to make reference to a crime listed in the EAW Framework Decision. The law enforcement stakeholders who expressed themselves in favour of access on a generalised access stated that consultation for a particular crime of the EAW Framework Decision is sufficiently specific and that therefore justification of the request is not necessary. Moreover, they argue that the reply to a consultation only informs about the availability of a matching fingerprint and is not sufficient to establish the identity of a person or to take law enforcement action. Law enforcement stakeholders in favour of a case-by-case approach referred to the VIS Council Decision that is based on a similar approach. In their view, each request should justify the reasons for consultation.

A number of law enforcement stakeholders explicitly requested to allow for mass comparison of fingerprints and unsolved latents against the fingerprints contained in the 'Eurodac' database. This would mean that a multitude of latents or fingerprints are forwarded to 'Eurodac' for comparison, for instance because a law enforcement authority wants to check all fingerprints of the unsolved cases of the last twelve months against the most recent data in 'Eurodac'. One of the arguments against bulk checks is that it consumes a lot of processing power of the system and could adversely affect the service to the current users of 'Eurodac'. It would require additional matching capacity and even more so when fast are urgently needed. Alternatively, limited comparison possibilities in periods of low-traffic could be considered.

8.2. Access in exceptional cases of urgency

The current response time of the 'Eurodac' system is sufficient in the eyes of most law enforcement stakeholders. Nonetheless, the expected raise of number of requests could negatively affect the technical capability of 'Eurodac' to respond quickly. For this reason 'Eurodac' should be capable to guarantee priority treatment of requests flagged as "urgent".

Moreover, to ensure the prompt handling of these exceptional cases of urgency from the moment of introducing a request for consultation until the moment that the reply is provided, law enforcement stakeholders support the view that *ex ante* verification of the individual request should be replaced by a verification immediately after the reply was provided (*ex post*) similar to the approach in the VIS Council Decision.

8.3. Ex ante verification

A number of law enforcement authorities acknowledge the need for a prior independent check on the lawfulness of the consultation of 'Eurodac'. They favour an independent *internal* legality check because they consider that consultation of data recorded in 'Eurodac' has no or if any, only a small impact on the privacy of the person involved, because the reply does not reveal the identity of a person. Among data protection authorities the issue was raised that ex ante verification should be regulated at the level of the judiciary.

8.4 Ex post data protection oversight

Law enforcement stakeholders generally acknowledge the need for data protection oversight of law enforcement access to 'Eurodac' by the national data protection authorities. Some of them stated that consultation of 'Eurodac' should be logged, to verify the legality later on.

Data protection authorities mentioned that their *ex post* data protection oversight is hampered by the lack of human resources and financial means which would moreover have an impact on the independence of these authorities.

8.5 The communication modes of requesting access to 'Eurodac'

A majority of law enforcement stakeholders hold the view that consultation of 'Eurodac' should be based on an electronic request addressed to a central access point. Some stated that access based on a written request should be allowed as fallback option in case electronic communication is impossible.

Stakeholders seem to agree that each Member State should designate an authority as National Central Access Point (hereafter referred to as NCAP) that would be the intermediary between the Member States' competent law enforcement authorities, authorised to consult 'Eurodac' and the Central Unit of 'Eurodac' that will carry out the consultation on their behalf. Such a national access point could be the existing national access points that functions as intermediary to 'Eurodac'. The NCAP would be a centralising contact point that would upload the fingerprints transmitted with the request for consultation in 'Eurodac', and it would be independent from existing contact points such as asylum or immigration authorities. One law enforcement stakeholder stated that the latter authorities should process the requests for consultation since they already have a secure network interface. Access via the existing 'Eurodac' national access points would have the practical advantage that connections are "ready to go" in terms of set up and security interface. Establishing law enforcement NCAPs

would not affect the search modalities provided for in the 'Eurodac' Regulation. Some law enforcement stakeholders favour direct access to 'Eurodac' by competent law enforcement authorities. Alternatively the existing national 'Eurodac' authorities could transmit requests to the Central Unit of 'Eurodac' on behalf of the law enforcement authorities and forward the replies to the requesting law enforcement authority.

9. The response times

The response time of 'Eurodac' to law enforcement consultations should be similar to that of requests from asylum authorities. The NCAP should communicate the reply immediately to the competent law enforcement authority. With regard to the time to obtain further biographical data in relation to a 'Eurodac' reply, law enforcement stakeholders mentioned this should be as short as possible, and not exceed 24 hours in normal circumstances and 8 hours in exceptional cases of urgency.

The current response time to a request to provide further biographical data is considered to be totally inadequate. Article 21 (5) of the Dublin II Regulation stipulates that the requested Member State shall be obliged to reply within six weeks. The time constraints to process an asylum request differ completely from those to respond effectively to crime and crime threats. Besides, law enforcement needs require that a special procedure with short response times would exist to deal with emergencies.

10. The data retention period

Data protection authorities consider that law enforcement authorities should specify (in each case) the period during which they want to retain the data. They consider that the current time limits in the 'Eurodac' Regulation are disproportional in relation to the purpose for which law enforcement authority envisage to use 'Eurodac' data and that the legislation should set the appropriate retention period.

Most law enforcement representatives prefer that the national law of the requesting Member State determines the retention period.

11. The onward processing to third States

Law enforcement stakeholders want to be able to transfer under certain conditions data retrieved from 'Eurodac' to third States because effective law enforcement sometimes calls for international cooperation.

Civil society stakeholders and national data protection authorities are strongly opposed to onward processing data to third States, in order to avoid that the data of an asylum seeker are transmitted to the State from which he fled. The opinion was raised that not only the issue of transfer of 'Eurodac' data and additional data to third States (including the State of origin of the asylum seeker) should be carefully looked into but also the onward processing in a domestic context.

12. Data security

Law enforcement stakeholders consider that the current data security requirements in the 'Eurodac' Regulation are adequate and sufficient. Nonetheless, a considerable number of them want to supplement these requirements with the relevant provisos of the Council

Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Some consider that the data security requirements in the VIS Council Decision are an attractive alternative

Data protection authorities stated that unauthorised access to 'Eurodac' and abuse of fingerprint data, but in particular of the further biographical data, should be prevented and be subject to sanctions.

13. Fundamental Rights

Civil society expressed serious concerns about the stigmatising effect that law enforcement access to 'Eurodac' would have. They fear that with this form of extended use of 'Eurodac', all asylum seekers will be automatically considered as potential crime suspects which would influence the way this (vulnerable) group of persons will be treated by society. As fingerprints are not available from all citizens in the same manner as from asylum seekers, the latter have an increased chance that they can be linked to and condemned for a crime on the basis of fingerprints via 'Eurodac' searches. Representatives of civil society emphasized the very vulnerable position of asylum seekers and the obligation to prevent that the State of origin would obtain or access information on the asylum applicant.

Law enforcement authorities however, pointed out that residents or citizens of Member States are more likely to have stable or known identities and are recorded in numerous databases. They refute that accessing fingerprint data of asylum seekers by them is causing stigmatisation since that it would be rather the consequence of the existence of the Dublin system itself. The fact that asylum seekers as a specific category of individuals are recorded in 'Eurodac' are setting them apart, not the fact that law enforcement would access these data. For that reason law enforcement consultation as such could not cause discrimination. Moreover, such consultation would not be disproportional or unduly interfere with the right to privacy if genuine law enforcement interests exist.

Some law enforcement stakeholders observed that 'Eurodac' is based on the consideration that each and every asylum seeker can potentially apply for asylum in different signatory States of the Dublin Regulation and that this assumption is sufficient ground to consider that it is necessary, proportional, and not excessive to coerce the taking of fingerprints.

However, not allowing or curtailing law enforcement access to 'Eurodac' heralds the view that inefficient data access leads to better protection of fundamental rights. Law enforcement stakeholders countered this point of view by pointing out that this leads to more crimes remaining unsolved and more expensive crime resolution. Paradoxically, inefficient crime resolution requires that law enforcement authorities access more personal data or more persons to establish whether or not relevant data exist. This causes a higher risk of infringement of privacy than efficient and straightforward access to databases would cause. Moreover, inefficient access demands more manpower of the law enforcement authorities and is more expensive. Furthermore, it was inferred that acceptance of the implicit argument that inefficient data access leads to better data protection is equally unfounded, unproven or unwarranted as claiming that access to all data should be free.

Annex 3

Administrative costs

Policy Option B:						**Tariff (€ per hour)**		**Time (hour)**		**Price (per action or equip)**	**Freq (per year)**	**Nbr of entities**	**Total nbr of actions**	**Total cost**	**Regulatory origin (%)**			
No.	Ass. Art.	Orig. Art.	Type of obligation	Description of required action(s)	Target group	i	e	i	e						Int	EU	Nat	Reg
1			notification	notification of the identity of the designated competent authorities level to the Commission.	Member States	25		5,00		125,00	1,00	27	27	3375,00		100%		
2			notification	notification of the national central access point (NCAP) to the Commission.	Member States	25		5,00		125,00	1,00	27	27	3375,00		100%		
3			listing	listing of the specialized units within the designated competent authorities at national level.	Member States	25		5,00		125,00	1,00	27	27	3375,00		100%		notif

4			Annual reporting	Annual reporting by the national data protection authorities	Member States	25		30,00		750,00	1,00	27	27	20250,00		100%		

The assumption is that there are 1760 working hours per year per person (8 hours * 20 days * 11 months).

Average employment costs in the EU-27 public administration: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (€20,35 in 2005). The 2005 figure has been rounded upwards, based on the assumption of economic growth and pattern over the preceding years and overheads of 10% have been added.

http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996,39140985&_dad=portal&_schema=PORTAL&screen=detailref&language=en&product=Yearlies_new_population&root=Y