

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 3.12.2008  
SEC(2008) 2981

**COMMISSION STAFF WORKING DOCUMENT**

*Accompanying the*

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]**

**Impact Assessment**

{COM(2008) 825 final}  
{SEC(2008) 2982}

## TABLE OF CONTENTS

1.	PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES...	4
2.	PROBLEM DEFINITION .....	5
2.1.	The context.....	5
2.2.	What are the problems to be addressed? .....	6
2.2.1.	Continuing late transmission of fingerprints.....	6
2.2.2.	Impossibility of filtering asylum claims by persons already enjoying international protection in a Member State .....	7
2.2.3.	Inefficient management of deletions of data.....	8
2.2.4.	Unclear specification of national authorities having access to EURODAC which hinders the monitoring role of the Commission and the EDPS .....	8
2.3.	How would the problem evolve, all things being equal?.....	9
2.4.	Does the EU have the right to act?.....	9
2.4.1.	Treaty basis .....	9
2.4.2.	Subsidiarity .....	9
2.4.2.1.	Transnational nature of the problem (‘necessity test’).....	9
2.4.2.2.	Value added test .....	10
2.4.3.	Proportionality .....	10
3.	POLICY OBJECTIVES.....	11
3.1.	General objectives.....	11
3.2.	Specific objectives .....	11
3.3.	Operational objectives.....	11
3.4.	Fundamental rights.....	12
4.	POLICY OPTIONS .....	12
4.1.	Status quo.....	12
4.2.	Action at EU level.....	12
5.	ANALYSIS OF IMPACTS OF THE POLICY OPTIONS .....	15
5.1.	Status quo:.....	15
5.2.	Action at EU level.....	16
6.	COMPARING THE OPTIONS .....	27
6.1.	Problem 1: Continuing late transmission of fingerprints .....	27
6.2.	Problem 2: Impossibility of filtering asylum claims by persons already enjoying international protection in a MS.....	27
6.3.	Problem 3: Inefficient management of deletions of data .....	28
6.4.	Problem 4: Unclear specification of national authorities having access to EURODAC, which hinders the monitoring role of the Commission and the EDPS .	28

7.	THE PREFERRED POLICY OPTION .....	29
7.1.	Assessment and considerations of proportionality and EU added value .....	29
7.1.1.	Proportionality .....	29
7.1.2.	Value added.....	30
8.	MONITORING AND EVALUATION .....	30
	ANNEX 1: GLOSSARY ON ASYLUM.....	31
	ANNEX 2: DESCRIPTION OF THE EURODAC SYSTEM.....	33
	ANNEX 3: ADMINISTRATIVE COSTS (including one-off investment costs).....	36

## Lead DG: Justice, Freedom and Security

AP reference number: 2008/JLS/156

### 1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

Since the beginning of its operations, four annual reports<sup>1</sup> have evaluated the activities of the EURODAC Central Unit. Moreover, the Commission services conducted a comprehensive evaluation of the Dublin system covering the first 3 years of operation of the EURODAC central system (2003-2005). The outcome of this exercise, the report on the evaluation of the implementation of the Dublin system (hereinafter: Evaluation Report), was published by the Commission in June 2007,<sup>2</sup> and forms an important basis for the present Impact Assessment. It has acknowledged the positive elements of the operation of the Dublin system, while at the same time pointing to shortcomings and problems in transposition.

Beyond the Evaluation Report, a number of other reports fed into this IA. A technical evaluation of DubliNet was carried out in 2005. The European Data Protection Supervisor (hereinafter: EDPS) has been inspecting the application of the Eurodac Regulation from a data protection point of view and issued an inspection report in July 2007<sup>3</sup> as well as an Activity Report covering the period 2005-2007.<sup>4</sup> In compliance with Article 20(2) of the Regulation, the EDPS drew up an in-depth security audit of the EURODAC system<sup>5</sup> in November 2007.

Additional input was received from Member States during and as a follow-up to the meeting of the EURODAC expert committee on 4-5 October 2007, where Member States discussed issue of delays in transmissions, endorsed the possibility of recording reasons for deletions and the technical functionality for mutual information about deletions affecting several Member States, and expressed an interest in obtaining hits on data on refugees (blocked at present).

During the formulation of the options, the IA on the Policy Plan on the Common European Asylum System<sup>6</sup> (prepared partly on the basis of the consultations on the Green Paper on the future Common Asylum System<sup>7</sup>) was used as an essential reference.

An Inter-Service Steering Group was convened on 20 June 2008, attended by DGs RELEX, SANCO and EAC.

---

<sup>1</sup> First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2004) 557; Second annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2005) 839; Third annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, SEC(2006) 1170; Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2006, SEC (2007) 1184.

<sup>2</sup> Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, SEC(2007) 742.

<sup>3</sup> Eurodac Supervision Coordination Group, Report of the first coordinated inspection, Brussels, 17 July 2007.

<sup>4</sup> Coordinated Supervision of Eurodac — Activity Report 2005-2007, 21 April 2008.

<sup>5</sup> 'Report on the EURODAC audit', document classified as EU RESTRICTED, short summary available at [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/07-11-09\\_Eurodac\\_audit\\_summary\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/07-11-09_Eurodac_audit_summary_EN.pdf).

<sup>6</sup> The objective of this policy plan is to lay down future legislative and non-legislative measures to be proposed by the Commission in order to complete the second phase of the Common European Asylum System.

<sup>7</sup> COM (2007)301.

The Commission's Impact Assessment Board (IAB) was consulted on the draft final Impact Assessment report and issued its opinion on 26 September 2008. Therein, the IAB considered that the present IA 'is overall of good quality and proportionate to the issues addressed in this initiative. (...) The policy objectives are concise and well articulated into general, specific and operational objectives. Linking them to the problem definition by means of footnotes makes the relationship between these sections of the report visible and can be considered as good practice.' The recommendations of the IAB were duly taken into account.

## 2. PROBLEM DEFINITION

### 2.1. The context

The Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities<sup>8</sup> (hereinafter: Dublin Convention) was signed on 15 June 1990 in Dublin. To facilitate the identification of third country nationals who fall under the scope of the Convention, a Community-wide system for the comparison of the fingerprints of asylum applicants was established, and named EURODAC.<sup>9</sup>

The conclusions of the Tampere European Council of 1999 state that a common European asylum system should include, in the short term, *inter alia*, a clear and workable determination of the state responsible for examining an asylum application lodged in a Member State by a third-country national. Rules thereto were laid down in the regulations which form the Dublin system: Council Regulation 343/2003/EC of 18 February 2003<sup>10</sup> (hereinafter: Dublin Regulation), its implementing Commission Regulation 1560/2003 of 2 September 2003<sup>11</sup> (which together replace the Dublin Convention), the Eurodac Regulation and its Implementing Regulation 407/2002/EC of 28 February 2002<sup>12</sup>.

The Dublin *acquis* is implemented by all Member States of the EU, as well as by Norway and Iceland. International agreements on the accession of Switzerland and Liechtenstein to the Dublin *acquis* were signed on 28 February 2008, and will enter into force as soon as they start applying the Schengen *acquis*. (In the present IA, the term 'Member States' is used to cover all states applying the Dublin *acquis*.)

In accordance with the *Policy Plan on Asylum — an integrated approach to protection across the EU*<sup>13</sup> which set out the main lines of action for the modification of the Regulation, the present Impact Assessment (IA) deals with problems identified in the Evaluation Report in order to update the system based on the experiences of the past 5 years of operations.

The Commission recalls that its legislative proposals in this field have to be compatible with the Charter of Fundamental Rights of the European Union (CFREU) and subject to an in-depth IA on fundamental rights.<sup>14</sup> 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, which applies to all cases where fingerprints are taken, and Article 18 guaranteeing the

---

<sup>8</sup> OJ C 254, 19.8.1997, p.1.

<sup>9</sup> For a description of the EURODAC system, cf. Annex 1.

<sup>10</sup> OJ L 50, 25.2.2003, p.1.

<sup>11</sup> OJ L 222, 5.9.2003, p.3.

<sup>12</sup> OJ L 62, 5.3.2002, p.1.

<sup>13</sup> COM(2008) 360.

<sup>14</sup> COM(2005) 172, 27.4.2005.

right to asylum, which applies to those cases where a claim for asylum is made.<sup>15</sup> Member States must respect fundamental rights when implementing Community obligations, such as those relating to the comparison of fingerprints of asylum applicants and others. This necessitates prompt and impartial investigation of any credible allegations of violations of fundamental rights. In addition, special attention should be devoted to the protection of the rights of the child (Article 24 of CFREU).

It has to be mentioned here that the long-term management of the second generation Schengen Information System (SIS II), the Visa Information System (VIS), EURODAC and other large scale IT systems in the area of Justice, Freedom and Security is subject to a separate IA currently under finalisation. This would, however, not impact on the issues analysed in the present IA.

## 2.2. What are the problems to be addressed?

Although the assessment of the activities of the EURODAC Central Unit (CU) as well as of the application of the Eurodac Regulation by the Member States has given general satisfaction, some provisions have been identified in the evaluation report of the Dublin system for improvement. On this basis, the following problems were identified.

### 2.2.1. *Continuing late transmission of fingerprints*

The Regulation in force provides only a very vague deadline for the transmission of fingerprints to the CU: Member States are required to ‘promptly take the fingerprints’ and ‘promptly transmit them’. In practice, in the absence of a strict deadline, and without any sanction as to non-compliance with the already vague deadline, delays in transmission of fingerprints were up to 30 days in some Member States in the past, while in 2007 the longest delay was almost 12 days. In some Member States, little progress has been observed since the installation of EURODAC, despite regular reminders by the Commission services through the annual activity reports and the meetings of the EURODAC expert committee.

A delay in transmissions may lead to results contrary to the responsibility principles laid down in the Dublin Regulation. Two kinds of scenarios may occur: First, the scenario of the so-called ‘**wrong hit**’. A third-country national lodges an asylum application in a Member State A (MS A), whose authorities take his/her fingerprints. While those fingerprints are still waiting to be transmitted to the Central Unit (category 1 transaction, hereinafter CAT1), the same person could already present him/herself in another Member State B (MS B) and ask again for asylum. If this MS B sends the fingerprints first, the fingerprints sent by the MS A would be registered in the Central database later than the fingerprints sent by MS B and would thus result in a hit from the data sent by MS B against the data sent by the MS A. Therefore, MS B would be determined as being responsible instead of MS A where the asylum application was lodged first.

Secondly, a so-called ‘**missed hit**’ can occur in the following scenario. A third-country national is apprehended in connection with an irregular border crossing and his/her fingerprints are taken by the authorities of the MS A he/she entered. While those fingerprints are still waiting to be transmitted to the Central Unit (category 2 transaction, hereinafter: CAT2), the same person can already present him/herself in MS B and lodge an asylum

---

<sup>15</sup> In addition, other rights guaranteed in the Charter of Fundamental Rights may be engaged depending on the circumstances. These include Article 6, the right to liberty and security; Article 7, the right to respect for private and family life; Article 19 prohibiting collective expulsions and upholding the principle of non-refoulement; Article 20, that everyone is equal before the law; Article 21 on non-discrimination as well as Article 47 as regards the right to a fair trial.

application. At that occasion, his/her fingerprints are taken by the authorities of MS B. If this MS B sends the fingerprints (CAT1) first, the Central Unit would simply register a CAT1 transaction, and hence MS B would handle the application (instead of MS A where he/she previously illegally entered the territory of the Member States). Therefore, when the CAT2 transaction of MS A arrives later on, a hit will be missed, since CAT2 data does not instigate a search against CAT1 data, but is only stored and CAT1 data transmitted afterwards are compared against it.

These scenarios are not only theoretical: in 2007, the Central Unit detected 60 ‘missed hits’, of which 57 were ‘in favour’<sup>16</sup> of the same Member State, and 233 ‘wrong hits’, 183 of which were against the same Member State.

### ***2.2.2. Impossibility of filtering asylum claims by persons already enjoying international protection in a Member State***

Under the Regulation in force, Member States have to ask the Central Unit to block the data of persons who are recognised as refugees. If a hit occurs against data of a person who was fingerprinted as an asylum seeker but whose data was later on blocked by a Member State because it recognised her/him as a refugee, the Central Unit records the hit for statistical purposes but sends a ‘no-hit’ reply to the Member State of origin.

The reason behind the formulation of this provision is that in accordance with Article 6(1) of the Data Protection Directive,<sup>17</sup> no data should be kept in a form which allows the identification of data subjects for longer than is necessary for the purposes for which data were collected.

The Regulation in force stipulates, however, that five years after Eurodac starts operations, a decision would be taken in accordance with the relevant provisions of the Treaty, as to whether the data relating to persons who have been recognised and admitted as refugees in a Member State should be stored and compared against CAT1 or should be erased in advance once they were recognised as refugees.

Statistics gathered by the EURODAC CU reveal that since the start of its activities (until 31.12.2007), 24 464 out of 1 005 323 data sets of asylum seekers (2.4%) were blocked. 414 out of the 24 464 blocked cases produced hits with subsequently transmitted CAT1 data. This means that 414 recognised refugees lodged a second asylum application in the same Member State as the one which granted the refugee status or in another Member State.<sup>18</sup> This phenomenon goes against the underlying principles of the Dublin system, since without being able to see the hits against the presently blocked cases, a new asylum procedure might start in another (or indeed the same) Member State consuming additional resources concerning a person who has already received protection from a Member State. The information that

---

<sup>16</sup> It was the same MS which, since it did not transmit the fingerprints in time, was *not* determined responsible.

<sup>17</sup> Directive 95/45/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995).

<sup>18</sup> From the point of view of the asylum-seeker or refugee, asylum shopping could in theory have the advantage of multiplying his/her chances of getting a certain level of protection. It has to be stressed though, that nevertheless, moving from one Member State to another entails financial costs for the asylum-seeker, as well as distress and uncertainty. The actual deterrent effect of the Dublin system from asylum shopping is largely dependent on the quality and level of information asylum-seekers are provided with.



Member State can obtain with the unblocking of these cases can of course be decisive in an asylum procedure.

### **2.2.3. *Inefficient management of deletions of data***

Under the Regulation in force, deletion of data is automatic from the database after 10 (CAT1) or 2 years (CAT2) respectively. *Advance erasure* of data by the Member State of origin (i.e. the Member State which entered the data of an asylum seeker or of a person apprehended when irregularly crossing an external border in the EURODAC Central database) is obligatory as soon as they become aware that a data subject has *acquired citizenship* of any Member State (both CAT1 and CAT2) and as soon as they become aware that the person has *left the territory* of the Member States or that he/she has been issued a *residence permit* (CAT2).

Another concern relates to the fact that Member States of origin are *often not aware that another MS of origin has deleted data* which corresponded to the fingerprint data it also entered into EURODAC at some point, and therefore should be subject to advance data erasure by all Member States of origin. Under the Regulation, it is obligatory to delete from the database all data on data subjects once they have been issued with a residence permit or granted citizenship or upon their departure from the EU territory. However, at present, Member States have no means to inform and be informed about advance data erasure by another Member State of origin, which means that they cannot apply the provisions on advance data erasure, and therefore some data might be stored in the database for a period that is longer than what would be justified for the purpose it was initially stored for. Compliance with the principle that ‘no data should be kept in a form which allows the identification of data subjects for longer than is necessary for the purposes for which data were collected’ cannot therefore be sufficiently monitored. This is a serious breach of data protection principles, which require data to be deleted when their storage is no longer necessary, and raises doubts about the compliance of Member States with data protection obligations.

### **2.2.4. *Unclear specification of national authorities having access to EURODAC which hinders the monitoring role of the Commission and the EDPS***

The Eurodac Regulation requests that Member States communicate to the Commission the list of authorities having access to data recorded in the Eurodac central database, for the purposes laid down in the Eurodac Regulation. From a data protection point of view, the relevant provisions in force can be considered too vague, since Member States may communicate an indefinite list of ‘authorities’ without any detail on the exact nature of the authority’s national competences and on the relevant departments. The Commission can only take note of the notifications and administer the list of authorities but cannot properly exercise its monitoring role.

The report of the first coordinated inspection of the EURODAC Supervision Coordination Group of 17 July 2007 identified as a problem the fact that the Regulation in force does not impose a particular structure or nature of the authority in charge of the management of EURODAC data. It furthermore recommended that national EURODAC authorities identify clearly the responsibilities of the different services using EURODAC in their respective Member States and that the number of authorities having access to the results of EURODAC searches must be limited.

Consequently, the EDPS and national data protection authorities (DPAs) rightly fear they cannot correctly assess whether all data protection rules are correctly applied in the context of the Eurodac Regulation, as they do not know who exactly is accessing data in each Member

State. This raises concerns regarding Member States' compliance with data protection principles.

### **2.3. How would the problem evolve, all things being equal?**

The existing EU measures cannot satisfactorily address the problems described above. Due to the complexity of the Dublin and EURODAC Regulations, there are still many possibilities for improvement and alignment of Member States' practices in implementation, on the basis of the mutual trust and cooperation underlying the Dublin system. The last few years of implementation have shown that there are limits to the use of practical cooperation among Member States striving to align their interpretation and practical understanding of the provisions of the Regulation (at the time adopted unanimously by the Council and therefore containing important compromises) and those limits have been reached. The fact that the Eurodac Regulation, as part of the first phase of the CEAS, was adopted by unanimous vote in the Council meant that on some points the final text is not sufficiently practice-oriented. This explains why, at present, alignment can prove to be difficult on certain issues (vague deadlines, lack of effective monitoring capacity for the Commission, etc.).

If no action at EU level is taken to address the difficulties described above, the problems identified will persist, since the present wording of the Regulation will not be sufficient to ensure a high standard of efficiency in supporting the application of the Dublin Regulation. Member States could decide to follow certain interpretations of their own which might interfere with the correct and uniform application of the Eurodac Regulation, thus resulting in serious divergences creating legal uncertainty.

### **2.4. Does the EU have the right to act?**

#### **2.4.1. Treaty basis**

Title IV of the EC Treaty ('TEC') on visas, asylum, immigration and other policies related to free movement of persons confers certain powers in these matters on the European Community. These powers must be exercised in accordance with Article 5 TEC, i.e. if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States and can, therefore, by reason of the scale or effects of the proposed action, be better achieved by the Community.

More specifically, the current legal basis for Community action regarding *criteria and mechanisms for determining which Member State is responsible for considering an application for asylum submitted by a national of a third country in one of the Member States*; is established in **Article 63 (1) (a) TEC**.

The reasons for a common intervention at EU level are clearly expressed in the paragraphs below, where the necessity test, based on the transnational nature of the problem, is provided.

#### **2.4.2. Subsidiarity**

##### *2.4.2.1. Transnational nature of the problem ('necessity test')*

The demand expressed by Member States and other relevant stakeholders during the wide consultation on the Green Paper on the CEAS and at various expert meetings shows the clear need for joint EU action to introduce a more efficient and consistent system for EURODAC.

The problems relating to asylum and refugee protection are transnational, so the EU is well placed to propose action in the framework of the Common European Asylum System (CEAS) to solve the problems described above regarding the Eurodac Regulation. Although a significant level of harmonisation was reached in the Regulation adopted in 2000, there is still

room for improvement in the support that Eurodac provides for implementing the Dublin Regulation. The need for EU action regarding the management of an EU database created to support the implementation of a Regulation on transnational movements of asylum seekers seems clear.

For the above-mentioned reasons, a coherent legal framework can only be established at Community level.

#### *2.4.2.2. Value added test*

Action at EU level will ensure that the problems identified are tackled with appropriate attention to the transnational nature of the problem.

Without appropriate measures at EU level, consistency with the evolved asylum *acquis* would not be ensured and important updates regarding some provisions on developments that have taken place since the adoption of the Regulation would not be possible.

Furthermore, better ensuring the respect of personal data would be more difficult.

#### **2.4.3. Proportionality**

The present IA aims at ensuring a more efficient and consistent system for EURODAC in the framework of the second phase of the Common European Asylum System (CEAS). Each suboption is assessed below so as to arrive at an ideal balance between practical value and efforts needed. Therefore, opting for EU action on the problems outlined above does not go beyond what is necessary to achieve the objective of solving those problems.

### **3. POLICY OBJECTIVES**

#### **3.1. General objectives**

3.1.1. *To enable more efficient determination of the Member State responsible for assessing asylum applications<sup>19</sup>*

3.1.2. *To better address data protection concerns*

#### **3.2. Specific objectives**

3.2.1. *To ensure truly prompt transmission of fingerprints<sup>20</sup>*

3.2.2. *To prevent asylum shopping by avoiding processing asylum claims from refugees<sup>21</sup>*

3.2.3. *To improve compulsory deletion of data<sup>22</sup>*

3.2.4. *To enable the Commission, the EDPS and national data protection authorities to effectively monitor the management of access to data in Eurodac by national authorities designated for the implementation of the Eurodac Regulation<sup>23</sup>*

#### **3.3. Operational objectives**

3.3.1. *To avoid ‘wrong hits’ and ‘missed hits’<sup>24</sup>*

3.3.2. *To ensure that asylum applications of refugees are not processed<sup>25</sup>*

3.3.3. *To ensure that data are deleted in circumstances specified by the current EURODAC Regulation<sup>26</sup>*

3.3.4. *To enable the Commission and EDPS to know who exactly is accessing data in each Member State<sup>27</sup>*

---

<sup>19</sup> Linked to one of the operational objectives of the IA on the Policy Paper on the CEAS: ‘to improve the system of allocation of responsibility between Member States (Dublin system, including EURODAC)’, connected to specific objectives No III., IV. and VI. therein: to enhance prompt and effective support to national asylum administrations, by promoting practical cooperation; to foster solidarity mechanisms for dealing with persons in need of protection, between Member States and between the EU and third countries; to prevent asylum shopping and secondary movements.

<sup>20</sup> Addresses the problems identified in 2.2.1 and the general objective 3.1.1.1.

<sup>21</sup> Addresses the problems identified in 2.2.2 and the general objective 3.1.1.1.

<sup>22</sup> Addresses the problems identified in 2.2.3 and the general objective 3.1.1.2.

<sup>23</sup> Addresses the problems identified in 2.2.4 and the general objective 3.1.1.2.

<sup>24</sup> Linked to the specific objective in 3.2.1.1.

<sup>25</sup> Linked to the specific objective in 3.2.1.2.

<sup>26</sup> Linked to the specific objective in 3.2.1.3.

<sup>27</sup> Linked to the specific objective in 3.2.1.4.

### 3.4. Fundamental rights

Positive and negative impacts on relevant fundamental rights have also been considered.

As the Eurodac Regulation is a technical instrument to aid effective implementation of some criteria of the Dublin Regulation, the impacts on fundamental rights have been assessed as regards the right to asylum<sup>28</sup> and the protection of personal data<sup>29</sup>.

## 4. POLICY OPTIONS

As will be clear from the problems listed above, the present IA considers a number of technical problems that are not necessarily closely interlinked.

Therefore, policy suboptions for each separate problem were drawn up and assessed. Consequently, the final preferred policy option is a combination of the preferred policy options for the individual suboptions. Given the different technical nature of the individual problems, there will be few if any synergies between the preferred policy suboptions.

In the framework of the IA on CEAS the policy option '*Further harmonisation of EU legislation associated with cooperation and harmonisation of best practices*' was chosen as the preferred option. The following policy options are designed in the framework of this general preferred policy option.

### 4.1. Status quo

If no EU action is taken, the imperfect application of some vague provisions of the Regulation will continue to undermine the effective support to the application of the Dublin Regulation to allocate responsibility for the assessment of asylum claims by Member States.

On the basis of experience in the past five years of operation of EURODAC, no Member State is expected to be motivated to apply Eurodac rules strictly if it knows that others do not and that the Commission does not have sufficient means of monitoring to enable it to take appropriate action. The Eurodac system is based on solidarity, which in practice often means Member States are only willing to make changes simultaneously with each other.

### 4.2. Action at EU level

#### 4.2.1. Problem 1: Continuing late transmission of fingerprints

#### **Option A) Facilitating the correct application of the Regulation by services provided by the CU**

If a Member State's delay in sending fingerprints exceeds a certain period of time (the recommended length of which could be based on a recommendation from the EURODAC expert committee), a warning message could be sent to the administrative mailbox of the

---

<sup>28</sup> Article 18 of the Charter of Fundamental Rights of the European Union provides that 'The right to asylum shall be guaranteed with due respect for the rules of the Geneva Convention of 28 July 1951 and the Protocol of 31 January 1967 relating to the status of refugees and in accordance with the Treaty on European Union and the Treaty on the Functioning of the European Union (hereinafter referred to as 'the Treaties').'

<sup>29</sup> Article 8 of the Charter of Fundamental Rights of the European Union stipulates that: '1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.'

Member State of origin reminding them of the recommended time-limit. This solution relies on the deterrent effect of regular reminders.

### **Option B) Using DubliNet**

Under this policy option Member States will be able to use DubliNet to notify problems with the transmission of fingerprints. In principle, bilateral cooperation among Member States can solve many issues of practical implementation. On some occasions, the delays in the sending of fingerprints can occur because of problems with the transmission facilities or because asylum seekers damage their fingertips in order to prevent their fingerprinting. Notifying through the secured bilateral communication tool, DubliNet<sup>30</sup>, if there are (these or other) problems with the transmission of fingerprints can in general provide solutions to solve complex cases where Member States dispute the outcome of the responsibility determination procedure due to late transmission of fingerprints.

### **Option C) Legislation — specifying a clearer deadline in the Regulation**

Drawing upon the consultation of Member States in the framework of the EURODAC expert committee on 4-5 October 2007, a possible solution could be to keep the time-limit somewhat flexible but at the same time to set an end date. Proposing a wording referring to the obligation to send data as soon as possible, but not later than a certain number of hours/days (the exact number of which is to be determined) could accommodate the need to set a final deadline but at the same time ensure that Member States which currently send data in a shorter period than the number of hours/days to be agreed upon as a deadline would still keep up their good performance.

#### ***4.2.2. Problem 2: Impossibility of filtering asylum claims by persons already enjoying international protection in a Member State***

##### **Option A) Legislation — *erase in advance***

Under this option, data on persons already granted a status would be erased in advance from the EURODAC database and therefore no hit would be possible to transmit should the same person apply for asylum again in a Member State.

##### **Option B) Legislation – *store and compare with CAT1***

###### **Option Ba) Store as CAT4**

Under this option, data on refugees would be retransmitted as a new category, i.e. CAT4, and stored separately from data on asylum seekers (CAT1). Member States would be obliged to erase in advance the initial CAT1 data as soon as they grant international protection to a previous asylum seeker. They would also be required to introduce a CAT4 transaction indicating ‘person received international protection’ for all persons they grant asylum to. This in practice would also include data on persons granted international protection who have not undergone a Dublin procedure, e.g. those who are granted asylum as a result of resettlement.

###### **Option Bb) Store and attribute a mark to data previously submitted as CAT1**

Upon indication by the Member State which has granted international protection to a third-country national whose data have been stored in EURODAC as a CAT1, the CU could attribute a mark meaning that the person has been recognised as eligible for international protection. This mark could be removed later if the person in question is no longer eligible for international protection.

---

<sup>30</sup> See Annex 1. The use of DubliNet is always compulsory except for the cases defined in Article 15(1) second subparagraph of Regulation 1560/2003/EC (Dublin Implementing Regulation).

#### **4.2.3. Problem 3: Inefficient management of deletions of data**

##### **Option A) Using DubliNet bilateral cooperation**

Member States could exchange data on deletions and reasons for them via DubliNet, the bilateral exchange tool connecting technical national access points (NAPs). Since it is run on an encrypted private network for public administrations, it satisfies confidentiality requirements. Use of this communication tool by Member States might enhance practical cooperation among Member States and ensure that they inform each other about the data that has to be deleted.

##### **Option B) Establishment of a centralised system based on DubliNet**

A technical evaluation of DubliNet carried out in 2005 outlined the possibility of a reconfiguration of the present DubliNet architecture (currently an exchange tool) into a centralised system, which would need to be established.

Such an upgrade was deemed useful for efficient handling of the growing number of transactions passing through DubliNet. It would also allow the creation of reliable automated statistics. The automatic collection of statistics based on the transactions between the NAPs (National Access Point servers), could help to solve difficulties in gathering reliable and complete statistics on the application of the Dublin Regulation.

##### **Option C) Automated information provided by the CU**

Data have to be deleted in advance from EURODAC if the change of the status of the data subject so requires (i.e. if he/she has obtained citizenship of a Member State, receives a residence permit, has left the territory of the Member States). In order to observe the principle of necessity and proportionality, all data on that person should be deleted from EURODAC. As explained in the problem definition, Member States are currently unaware of each others' deletions, which might mean that they ought to delete data they entered on the same person. Under this option however, when a Member State deletes fingerprints (along with the other associated data) which produce hits with the fingerprints that were entered in EURODAC by the other Member States of origin, an automated message could be sent to these latter Member States. This would allow them to delete data whose retention in EURODAC is no longer justified.

#### **4.2.4. Problem 4: Unclear specification of national authorities having access to EURODAC, which hinders the monitoring role of the Commission and the EDPS**

##### **Option A) Legislation on obligation to notify relevant details of the designated authority to the Commission**

Legislation giving the Commission the chance to monitor the designation of authorities, by requiring Member States' official notifications to include details of the exact nature of the authority's national competences, and of the relevant departments within the authority that deal with the application of the Eurodac Regulation.

##### **Option B) Exchange of information on relevant details of the designated authority in the framework of the EURODAC expert committee**

Following the general notification according to the Regulation in force, Member States can regularly exchange information including details of their designated authorities in the framework of the EURODAC expert committee.

## 5. ANALYSIS OF IMPACTS OF THE POLICY OPTIONS

As will be clear from the problems listed above, the present IA considers a number of technical problems that are not necessarily closely interlinked.

Therefore, policy suboptions for each separate problem were drawn up and assessed. Consequently, the final preferred policy option is a combination of the preferred policy options for the individual suboptions. Given the different technical nature of the individual problems, there will be few if any synergies between the preferred policy suboptions.

### Rating of impacts:

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. Status quo:

Policy Option A: Status quo		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Relevance</b>		
<i>To ensure truly prompt transmission of fingerprints</i>	0	Maintaining the status quo would prevent the better and quicker allocation of responsibility for the assessment of asylum claims. Missed and wrong hits would continue to occur and create false determination of responsibility.
<i>To prevent asylum shopping by avoiding processing asylum claims from refugees</i>	0	The obligation to take the decision whether data on refugees should be stored and run a comparison against CAT1 or be erased in advance is stipulated by the Regulation. Therefore failing to make this decision (due five years after EURODAC started operation, i.e. on 15 January 2008) would be in breach of the Regulation. The decision is best placed in a new provision of the modified Regulation.



Policy Option A: Status quo		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<i>To improve the compulsory deletion of data</i>	0	Should no changes be made to the current practices, an opportunity would be missed to improve the application of the Dublin Regulation, since MSs would remain unaware of the need to delete data which have been deleted by another MS of origin. If there is no possibility for MSs to indicate the reasons for deletions, national data protection authorities will still be unable to effectively monitor the observance of the rules on deletions. Both cases raise data protection concerns, since data would be kept in the database longer than is justified.
<i>To enable the Commission, the EDPS and national data protection authorities to effectively monitor the management of access to data in Eurodac by national authorities designated for the implementation of the Eurodac Regulation</i>	0	Data protection concerns would continue to prevail as to the exact number and nature of staff having access to EURODAC on behalf of the responsible authorities designated on the basis of the Regulation in force.
<b>Transposition feasibility</b>		
- Under existing treaty	0	The policy option does not provide for further measures to be transposed and therefore there are no difficulties or risks in this sense.
- Under new treaty	0	The policy option does not provide for further measures to be transposed and therefore there are no difficulties or risks in this sense.
Implementation costs	0	No additional financial and administrative costs would be incurred if preserving the status quo.

## 5.2. Action at EU level

### 5.2.1. Problem 1: Continuing late transmission of fingerprints

Policy Option A: Facilitating the correct application of the Regulation by services provided by the CU		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Expected Impacts</b>		
<i>To ensure truly prompt transmission of fingerprints</i>	√√√	This solution improves compliance with the Dublin Regulation by reminding MSs of the need to promptly take and send the fingerprints. The time after which a reminder would be sent by the CU would be set by the EURODAC expert committee.
impacts on fundamental rights	√√	<i>Right to asylum</i> A successful scheme to deter MSs from late transmission would indirectly benefit asylum seekers, since (with the decline in the numbers of wrong and missed hits) a more punctual and earlier determination of responsibility would be possible, therefore they would have their claim effectively assessed earlier and the notion of 'refugees in orbit' would be further reduced. <i>Protection of personal data</i> No significant impact, as the same data would be stored, but from a different period on.
administrative costs for the Commission	0	No administrative burden on the COM is expected, as this option entails changes in IT systems and from there on everything is automated.
administrative costs for MS	0	No administrative burden on the COM is expected, as this option

Policy Option A: Facilitating the correct application of the Regulation by services provided by the CU		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
		entails changes in IT systems and from there on everything is automated.
costs of implementation (i.e. all costs)	-√√	At the time of implementation (first year): EUR 27 000–40 000 for changes to the central EURODAC system (based on 20–30 days of work for contractor and 100–150 hours for COM).
Consistency with the asylum <i>acquis</i>	√√√	This solution entails no change in the legal framework, but is consistent with the Regulation.
<b>Implementation feasibility</b>	√√√	No difference of impact between the two treaties. Since this solution entails technical changes in the system and no changes in the legal framework, no difference of impact is expected under the two treaties.

Policy Option B: Using DubliNet		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Expected Impacts</b>		
<i>To ensure truly prompt transmission of fingerprints</i>	√	Bilateral information exchange effectively enhances cooperation in concrete cases. However, communication of every problem of transmission (system downtime, impossibility to fingerprint the applicant, e.g. because his fingers are damaged) can overburden the system. Therefore, the principle of proportionality is not observed by choosing this option.
impacts on fundamental rights	√√	<i>Right to asylum</i> A successful scheme of targeted bilateral cooperation would indirectly benefit asylum seekers, since (with the decrease of the numbers of wrong and missed hits) a more punctual and earlier establishment of responsibility would be possible, therefore they would have their claim effectively assessed earlier and the notion of 'refugees in orbit' would be further reduced.  <i>Protection of personal data</i> There is a risk that DubliNet may be controlled or monitored differently from EURODAC, with the problems that this will entail for citizens' data protection rights.
administrative costs for the Commission	0	No changes to the development or configuration of the system would be needed.
administrative costs for MS	-√	Some administrative burdens for the MSs are expected (additional allocation of staff), as this option entails action by the MSs. +/- EUR 145 000 (each MS would handle about 200 cases, each case would take about one hour of work).
costs of implementation (i.e. all costs)	-√	EUR 5 500–7 500 for the development of new DubliNeT forms by a contractor and 50 hours of work for COM to distribute the forms, manage the contractor and test the forms.
consistency with the asylum <i>acquis</i>	√√√	This solution entails no change in the legal framework, but is consistent with the Regulation.
<b>Implementation feasibility</b>	√√√	No difference of impact between the two treaties. Since this solution entails technical changes in the system and no changes in the legal framework, no difference of impact is expected under the

Policy Option B: Using DublinNet		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact

two treaties.

Policy Option C: Legislation – specifying a clearer deadline in the Regulation		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact

**Expected Impacts**

<i>To ensure truly prompt transmission of fingerprints</i>	√√√	With a precise deadline laid down by the Regulation, MSs will comply better with their obligations to take and transmit fingerprints in time to allow determination of the MS responsible. Since the deadline would be clear and objective, the Commission would be able to chase up any mass delays by MS by launching infringement proceedings.
impacts on fundamental rights	√√√	<i>Right to asylum</i> Ensuring swifter transmissions would benefit asylum seekers, since (with fewer wrong and missed hits) a more punctual and earlier determination of responsibility would be possible, therefore they would have their claim effectively assessed earlier and the notion of ‘refugees in orbit’ would be further reduced. <i>Protection of personal data</i> Current data protection will remain applicable.
administrative costs for the Commission	0	No changes to the development or configuration of the system would be needed.
administrative costs for MS	-√	Minor administrative burdens can be expected for those MSs that do not currently comply with the vague deadline definition (‘promptly transmit’) in the Regulation in force. They will have to speed up their national practices.
costs of implementation (i.e. all costs)	-√	Should this option be retained, minor cost increases may be expected for some MSs.
consistency with the asylum <i>acquis</i>	√√√	This solution would specify the deadline, to allow better application of the Regulation and better compliance with its original intention and spirit. Including a clearer time-period for the data transmission deadline would make determination of responsibility more accurate. As explained above, excessive delays in taking and transmitting fingerprints can have consequences leading to results contrary to the objectives of the Dublin Regulation. By pursuing the present policy objective, wrong hits and missed hits could be reduced or eliminated. Member States systematically missing the deadline could face infringement proceedings.
<b>Implementation feasibility</b>	√√√	No difference of impact between the two treaties. Some MSs are expected to be somewhat reluctant to agree on a more specific deadline. The European Parliament is expected to favour a more specific deadline.

**5.2.2. Problem 2: Impossibility of filtering asylum claims by persons already enjoying international protection in a Member State**

Policy Option A: Legislation – erase in advance		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact

Policy Option A: Legislation – <i>erase in advance</i>		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact

**Expected Impacts**

<i>To prevent asylum shopping by avoiding processing asylum claims from refugees</i>	0	If this option is retained, MSs would be expected to erase in advance the data they previously entered in the system as soon as they grant international protection <sup>31</sup> to the person in question. This would mean that MSs subsequently transmitting data to EURODAC about the same person would not receive a hit response and therefore would (continue to) be unaware of the fact that the person in question in fact already enjoys international protection in a MS.
impacts on fundamental rights	√	<p><i>Right to asylum</i></p> <p>Since MSs would <i>continue to be unaware</i> (as is the case at present) if a person applying to their national administrations for international protection has in fact already been granted it by a MS, they would have to continue to devote resources also to applicants resorting to asylum shopping. Therefore those with genuine international protection needs might receive less support and attention.</p> <p><i>Protection of personal data</i></p> <p>Data on refugees are not primarily destined to be stored in EURODAC, whose purpose is to establish the MS responsible. Deleting data would therefore be favourable for data protection reasons.</p>
administrative costs for the Commission	0	Minor changes might have to be introduced in the configuration of the system.
administrative costs for MS	0	No changes are expected in the administrative burden on MSs; they would just have to erase relevant data instead of blocking them as currently required.
costs of implementation (i.e. all costs)	-√	EUR 17 000–30 000, 10–20 days for a service supplier to change the EURODAC system and 100–150 hours for COM to manage contract and test.
consistency with the asylum <i>acquis</i>	√√√	<p>Since the decision to choose between the two options is called for by the Regulation itself, this option is by definition consistent with the asylum <i>acquis</i>.</p> <p>However, the Commission would be deprived of the (presently available) possibility to produce ‘statistics on hits against blocked cases’, i.e. to monitor whether the information provided by MSs to asylum seekers on the operation of the Dublin system has a deterrent effect on asylum shopping.<sup>32</sup></p>
<b>Implementation feasibility</b>	-√√	No different impact is expected under the two treaties. MSs are expected to be reluctant to erase data on refugees, since in the framework of the EURODAC expert committee they expressed a clear interest in receiving the hits against the fingerprints they blocked. The opinion of the European Parliament is not yet known.

Policy Option B: Legislation – <i>store and compare with CATI</i>		
Option Ba) Store as CAT4		

<sup>31</sup> On the enlargement of the scope of the Dublin Regulation to cover also subsidiary protected persons, cf. the IA on the amendments to the Dublin Regulation.

<sup>32</sup> ‘Asylum shopping’ is a form of secondary movement, where the third-country national, despite the fact that they have already received international protection, applies again for asylum in the same or in another Member State.

Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Expected Impacts</b>		
<i>To prevent asylum shopping by avoiding processing asylum claims from refugees</i>	√√√	<p>Checking of whether a person has been already granted refugee status is not <i>expressis verbis</i> one of the criteria to allocate responsibility under the Dublin Regulation. However, this Regulation is based on the principle that while only one MS is responsible for the assessment of the asylum claim, the same MS hold this responsibility even after the determination of his case (i.e. the responsible MS takes back the person whose application it rejected). Knowing that a person is already enjoying international protection in a MS is of course decisive for national asylum authorities.</p> <p>However, storing data on all persons granted international protection including those who have not undergone a Dublin procedure (e.g. those who are granted asylum as a result of resettlement) would be disproportionate from both a data protection and an efficiency point of view.</p>
impacts on fundamental rights	√√	<p><i>Right to asylum</i></p> <p>Since MSs would know if a person already enjoying international protection in a MS applies for it again, MSs would have to devote less resources to those who recourse to asylum shopping, therefore those with genuine international protection needs would have the chance to receive more support and attention.</p> <p><i>Protection of personal data</i></p> <p>Data on refugees are not primarily destined to be stored in EURODAC, whose purpose is to establish the MS responsible. Storing and searching these data might therefore raise data protection concerns. Storing data would imply a change of purpose, which needs to be justified as necessary and proportionate, in accordance with the law.</p>
administrative costs for the Commission	0	No administrative cost for COM.
administrative costs for MS	-√√	EUR 500 000 (1 hour per case, 20 000 cases per year).
costs of implementation (i.e. all costs)	-√√√	EUR 460 000–500 000. (80 to 120 days by contractor to modify EURODAC system, 300 to 450 hours for COM to manage contract and test, 10 000 per MS for changes to local IT systems and 100 hours per MS to manage contract and test).
consistency with the asylum <i>acquis</i>	√	<p>Since the decision to choose between the two options is called for by the Regulation itself, this option is by definition consistent with the asylum <i>acquis</i>.</p> <p>Storing data on all persons who receive international protection as CAT4 'person received international protection', would not directly serve the application of the Dublin Regulation. However, it would facilitate decision-making by national asylum authorities in conformity with the Qualification and Procedures Directives.<sup>33</sup></p>
<b>Implementation feasibility</b>	√√	No difference of impact between the two treaties. MSs (in the framework of the EURODAC expert committee) expressed a clear interest in receiving hits against the fingerprints they blocked. The opinion of the European Parliament is not yet known.

<sup>33</sup> Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third-country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted, Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in Member States for granting and withdrawing refugee status.

Policy Option B: Legislation – store and compare with CATI		
Option Bb) Store and attribute a mark to data previously submitted as CATI		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact

**Expected Impacts**

<i>To prevent asylum shopping by avoiding processing asylum claims from refugees</i>	√√	Checking whether a person has already been granted refugee status is not <i>expressis verbis</i> one of the criteria for allocating responsibility under the Dublin Regulation. However, this Regulation is based on the principle that while only one MS is responsible for the assessment of the asylum claim, the same MS holds this responsibility even after the determination of the case (i.e. the responsible MS takes back the person whose application it rejected). Knowing that a person is already enjoying international protection in a MS is of course decisive for national asylum authorities. It is to be noted that of course with the extension of the scope of the Regulation, data on persons having received subsidiary protection status will also be marked. On the extension of the scope of the Dublin Regulation to cover persons enjoying subsidiary protection, cf. the IA on the Dublin Regulation. The analysis of the relevant figures indicates that the number of 24 464 blocked data of asylum applicants is far too low compared to the number of refugees recognised by Member States between 2003 and 2007, i.e. approximately 100 000 persons. <sup>34</sup>
impacts on fundamental rights	√√	<i>Right to asylum</i>  Since MSs would know if a person already enjoying international protection in a MS applies for it again, MSs would have to devote fewer resources to applicants who resort to asylum shopping, therefore those with genuine international protection needs would have the chance to receive more support and attention.  <i>Protection of personal data</i>  Data on refugees are not primarily destined to be stored in EURODAC, whose purpose is to establish the MS responsible. Storing and searching these data might therefore raise data protection concerns.
administrative costs for the Commission	0	No administrative cost for COM.
administrative costs for MS	0	No difference in the administrative burden on MSs would occur, since they will have to perform the same number of operations, only of a different nature (marking instead of blocking).
costs of implementation (i.e. all costs)	-√√	Should this option be retained, costs would be incurred for the Commission and MS. Commission: EUR 59 000–110 000 (45 to 90 days for contractor to change EURODAC system and 200 to 300 hours for COM to manage contract and test).  MS: EUR 370 000. (EUR 10 000 per MS for contractor to change IT systems and 100 hours for each MS to manage contract and test).

<sup>34</sup>

This means that Member States have correctly applied the EURODAC Regulation (i.e. proceeded with blocking data on recognised refugees) only in approximately 20% of the cases. (NB: data on recognitions in MSs as well as in Norway and Iceland have to be modified according to the years when the MSs which joined the EU in the two last waves of enlargement (10 MSs on 01.05.2004, 2 MSs on 01.01.2007) were not yet applying the Dublin and Eurodac *acquis*. It also has to be noted that contrary to recognition figures, data on asylum seekers are transmitted to EURODAC only concerning those above the age of 14.) In order to effectively assist MSs by providing representative information on persons already enjoying international protection, MSs would need to systematically comply with their obligation to administer data on persons who are recognised.

Policy Option B: Legislation – store and compare with CATI		
Option Bb) Store and attribute a mark to data previously submitted as CATI		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
consistency with the asylum <i>acquis</i>	√√	<p>Since the decision to choose between the two options is called for by the Regulation itself, this option is by definition consistent with the asylum <i>acquis</i>.</p> <p>As soon as a MS grants international protection to a third-country national whose data have been stored in EURODAC as a CATI, the CU would attribute a mark meaning that the person was recognised as eligible for international protection. This solution conforms with the principles of the Dublin Regulation and it would also facilitate decision-making by national asylum authorities in conformity with the Qualification and Procedures Directives.</p>
Implementation feasibility	√√	No difference of impact is expected under the two treaties. MSs (in the framework of the EURODAC expert committee) expressed a clear interest in receiving hits against the fingerprints they blocked. The opinion of the European Parliament is not yet known.

### 5.2.3. Problem 3: Inefficient management of deletions of data

Policy Option A: Using DubliNet bilateral cooperation		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Expected Impacts</b>		
To improve the compulsory deletion of data	√	MSs could exchange data via DubliNet on deletions and the reasons for them.. This option is expected to enhance practical cooperation between MSs and to help ensure that MSs inform each other about the data to be deleted. However, this option would not allow the Commission to draw up proper statistics on the breakdown of cases by reasons for deletion. It would also be problematic from a proportionality point of view, since it would run the risk of overburdening DubliNet.
impacts on fundamental rights	- √√	<p><i>Right to asylum</i></p> <p>No impact.</p> <p><i>Protection of personal data</i></p> <p>Data subjects whose data no longer need to be included in EURODAC (for reasons triggering advance erasure, i.e. obtaining citizenship, receiving a residence permit, leaving the territory of the MSs) might be still kept in the system, since keeping other MSs informed via DubliNet itself might not in all cases involve actual erasure from EURODAC. This is due to the fact that even though in concrete cases MSs might know or assume which other MSs had also entered data on the same subject, this knowledge/assumption can hardly be perfect. Moreover, if this solution were selected, the standard of protection of personal data would be lower than in the present EURODAC framework.</p>
administrative costs for the Commission	0	No administrative cost for COM.
administrative costs for MS	-√√	+/- EUR 750 000 per year (6 000 deletions — 1 hour — 5 MS per deletion)
costs of implementation (i.e. all costs)	-√√	EUR 5 500–7 500 (2 000–4 000 for creating forms and 50 hours for COM to manage contract and test).

Policy Option A: Using DubliNet bilateral cooperation		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
consistency with the asylum <i>acquis</i>	√	As a technical solution for information exchange on the technical level, this option is consistent with the Eurodac Regulation and aims to facilitate the application of the Dublin Regulation, by using the secured bilateral communication tool (DubliNet) established by the Implementing Regulation (1560/2003/EC) <sup>35</sup> of that Regulation. As such, it is consistent with the asylum <i>acquis</i> .
<b>Implementation feasibility</b>	-√√	No difference of impact is expected under the two treaties. MSs are expected to be strongly opposed to this option, since they would experience a significant increase of workload for their national administration. The opinion of the European Parliament is not yet known.

Policy Option B: Establishment of a centralised system based on DubliNet		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Expected Impacts</b>		
To improve the compulsory deletion of data	√√	MSs could exchange data on deletions and the reasons for them via a centralised system based on DubliNet, which would need to be established. This option is expected to greatly encourage practical cooperation among MSs and might also ensure that MSs inform each other about the data that need to be deleted, and allow the Commission to draw up proper statistics on the breakdown of cases by reasons for deletion. However, serious proportionality concerns might arise from both data protection and cost-effectiveness points of view.
impacts on fundamental rights	-√√√	<i>Right to asylum</i> No impact. <i>Protection of personal data</i> Since the data exchanged through DubliNet include extensive personal information, significant data protection concerns arise concerning its creation.
administrative costs for the Commission	-√√√	EUR 366 000 (3 persons for support and administration — 220 days — 7.5 hours/day).
administrative costs for MS	-√√√	EUR 150 000 (based on 6 000 deletions and one hour for each case).
costs of implementation (i.e. all costs)	-√√√	First year of operations: COM cost of EUR 500 000–900 000; MS cost of EUR 600 000–900 000.
consistency with the asylum <i>acquis</i>	√	The automatic collection of statistics based on transactions between the NAPs would help to solve difficulties in gathering reliable and complete statistics on the application of the Dublin Regulation. However, the establishment of a new system would require a separate IA.
<b>Implementation feasibility</b>	-√√√	No difference of impact is expected under the two treaties.

<sup>35</sup> Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 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.



Policy Option B: Establishment of a centralised system based on DubliNet		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact

However, when reacting to the technical evaluation of DubliNet carried out in 2005 (which outlined the possibility of a reconfiguration of the DubliNet architecture on the basis of a centralised system), MSs reached no consensus on whether to endorse this option. The opinion of the European Parliament is not yet known.

Policy Option C: Automated information provided by the CU		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact

#### Expected Impacts

To improve the compulsory deletion of data	√√√	When a MS deletes fingerprints (along with the other associated data) which produce hits with the fingerprints entered in EURODAC by the other MSs of origin, an automated message could be sent to these latter MSs. This option is expected to ensure that the data to be deleted is effectively deleted by MSs. This option also requires legislation specifying the relevant technical functionality (automated information to MSs of origin) in the Eurodac Regulation. Choosing this option would not detract from the Commission's ability to launch infringement proceedings, where appropriate.
impacts on fundamental rights	√√√	<i>Right to asylum</i> No impact. <i>Protection of personal data</i> Data subjects whose data no longer need to be included in EURODAC (for reasons triggering advance erasure, i.e. obtaining citizenship, receiving a residence permit, leaving the territory of the MSs) would reasonably be expected to be effectively deleted.
administrative costs for the Commission	0	No administrative cost for COM.
administrative costs for MS	-√	EUR 45 200 per year for MS (based on 200 cases per country and 0.3 hours per case).
costs of implementation (i.e. all costs)	-√	For COM: EUR 66 000–95 000 (40–60 days for contractor to change the EURODAC system and 350–450 hours for COM to manage contract and test). For MS: EUR 370 000 (EUR 10 000 EUR per MS for contractor to change IT systems and 100 hours to manage contracts and test).
consistency with the asylum <i>acquis</i>	√√√	The application of the Dublin Regulation would be efficiently ensured.
<b>Implementation feasibility</b>	√√√	No difference of impact is expected under the two treaties. Member States are expected to be favourable to the development of the technical platform enabling them to be informed about deletions. The opinion of the European Parliament is also expected to be favourable.

#### 5.2.4. Problem 4: Unclear specification of national authorities having access to EURODAC, which hinders the monitoring role of the Commission and the EDPS

Policy Option A: Legislation on obligation to notify relevant details on the designated authority to the Commission		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Expected Impacts</b>		
<i>To enable the Commission, the EDPS and national data protection authorities to effectively monitor the management of access to data in EURODAC by national authorities designated for the implementation of the EURODAC Regulation</i>	√√√	If, in their official notification, MS gave details of the exact nature of the authority's national competences and of the relevant departments in the authority dealing with the application of the EURODAC Regulations, it would enable proper monitoring of MSs' activities concerning EURODAC.
impacts on fundamental rights	√√√	<i>Right to asylum:</i> No impact.  <i>Protection of personal data</i> Better definition of responsible authorities would ensure the observance of the rights of the data subjects and facilitate effective supervision by national data protection authorities.
administrative costs for the Commission	0	No administrative burden and no costs would be incurred for the Commission.
administrative costs for MS	0	No additional administrative burden would be incurred for the MSs, since the details required would be notified in the same way as any notification currently provided of changes in the structure of national administrations.
costs of implementation (i.e. all costs)	0	This option would involve no administrative costs for either the Commission or the MSs.
consistency with the asylum <i>acquis</i>	√√√	A better definition of responsible authorities would ensure observance of the data protection and data security rules outlined in the Regulation.
<b>Implementation feasibility</b>	√√√	No difference of impact is expected under the two treaties. MSs are expected to endorse this option. The opinion of the European Parliament and the EDPS is also expected to be favourable.

Policy Option B: Exchange of information on the relevant details on the designated authority in the framework of the EURODAC expert committee		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
<b>Expected Impacts</b>		
<i>To enable the Commission, the EDPS and national data protection authorities to effectively monitor the management of access to data in Eurodac by national authorities designated for the implementation of the Eurodac Regulation</i>	√√	Following the general notification procedures under the Regulation in force, MSs can regularly exchange details of their designated authorities in the framework of the EURODAC expert committee. Cooperation mechanisms could be established between this committee and the EURODAC EDPS-DPAs <sup>36</sup> Coordination Meetings.

<sup>36</sup> National data protection authorities.

Policy Option B: Exchange of information on the relevant details on the designated authority in the framework of the EURODAC expert committee		
Assessment Criteria	Rating	Motivation of the rating and aspects of the policy option necessary to achieve the impact
impacts on fundamental rights	√	<p><i>Right to asylum</i></p> <p>No impact.</p> <p><i>Protection of personal data</i></p> <p>This option would be expected to improve the flow of information from the MSs to the Commission and the EDPS and <i>vice versa</i> on the exact procedures for access to EURODAC information by national authorities. However it would provide no legal certainty as regards respect for the rights of the data subjects and would not facilitate effective supervision.</p>
administrative costs for the Commission	-√	EUR 55 000 (COM presence and preparation for 2 meetings and travel expenses for 2 expert meetings with all MS)
administrative costs for MS	0	No cost, since participation in the meetings of the EURODAC expert committee is reimbursed by COM.
costs of implementation (i.e. all costs)	0	Should this option be retained, no administrative costs would arise for either the Commission or the MSs.
consistency with the asylum <i>acquis</i>	√	Some indication as to the organisation of the responsible authorities would help the Commission to monitor the practices of MSs in ensuring compliance with the data protection and data security rules outlined in the Regulation.
<b>Implementation feasibility</b>	-√√√	No difference of impact is expected under the two treaties. MSs might have reservations about this option. The opinion of the EDPS is expected to be unfavourable, while that of the European Parliament is not yet known.

## 6. COMPARING THE OPTIONS

### 6.1. Problem 1: Continuing late transmission of fingerprints

	Policy Option A	Policy Option B	Policy Option C
<i>To ensure truly prompt transmission of fingerprints</i>	√√√	√	√√√
impacts on fundamental rights	√√	√√	√√√
administrative costs for the Commission	0	0	0
administrative costs for MS	0	-√	-√
costs of implementation (i.e. all costs)	-√√	-√√	-√
consistency with the asylum <i>acquis</i>	√√√	√√√	√√√
implementation feasibility	√√√	√√√	√√√

*Policy Option C is the preferred suboption.*

### 6.2. Problem 2: Impossibility of filtering asylum claims by persons already enjoying international protection in a MS

	Policy Option A	Policy Option Ba	Policy Option Bb
<i>To prevent asylum shopping by avoiding processing asylum claims from refugees</i>	0	√√√	√√√
impacts on fundamental rights		√√	√√
administrative costs for the Commission	0	0	0
administrative costs for MS	0	-√√	0
costs of implementation (i.e. all costs)	-√	-√√√	-√√
consistency with the asylum <i>acquis</i>	√√√	√	√√√
implementation feasibility	-√	√√	√√√

*Policy Option Bb is the preferred suboption.*

### 6.3. Problem 3: Inefficient management of deletions of data

	Policy Option A	Policy Option B	Policy Option C
To improve the compulsory deletion of data	√	√√	√√√
impacts on fundamental rights	-√√	-√√√	√√√
administrative costs for the Commission	0	-√√√	0
administrative costs for MS	-√√√	-√√√	-√
costs of implementation (i.e. all costs)	-√	-√√√	-√
consistency with the asylum <i>acquis</i>	√√√	√	√√√
implementation feasibility	-√√√	-√	√√√

*Policy Option C is the preferred suboption.*

### 6.4. Problem 4: Unclear specification of national authorities having access to EURODAC, which hinders the monitoring role of the Commission and the EDPS

	Policy Option A	Policy Option B
<i>To enable the Commission, the EDPS and national data protection authorities to effectively monitor the management of access to data in Eurodac by national authorities designated for the implementation of the Eurodac Regulation</i>	√√√	√√
impacts on fundamental rights	√√√	√
administrative costs for the Commission	0	-√
administrative costs for MS	0	0
costs of implementation (i.e. all costs)	0	0
consistency with the asylum <i>acquis</i>	√√√	√
implementation feasibility	√√√	-√√√

*Policy Option A is the preferred suboption.*

## 7. THE PREFERRED POLICY OPTION

With a view to further harmonisation of national laws and cooperation between Member States to allow a more effective and efficient implementation of the legislation, a combination of **policy options 1C, 2Bb, 3C, 4A and 5C** has been identified as the preferred policy option on the basis of the comparative analysis carried out in the previous section.

Preferred option: combination of policy options 1C, 2Bb, 3C and 4A		
Assessment Criteria	Rating	Reasons for the rating and aspects of the policy option necessary to achieve the impact
<b>Relevance</b>		
<i>To ensure truly prompt transmission of fingerprints</i>	√√√	With a precise deadline laid down in the Regulation, MSs will better conform to their obligations to take and transmit fingerprints in time to allow determination of the MS responsible. Since the deadline would be clear and objective, the Commission would be able to chase up any mass delays by MS by launching infringement proceedings.
<i>To prevent asylum shopping by avoiding processing asylum claims from refugees</i>	√√√	Knowing that a person is already enjoying international protection in a MS is decisive for national asylum authorities, enabling them to save the time and resources that would otherwise be used to deal with these claims. .
<i>To improve the compulsory deletion of data</i>	√√√	When a MS deletes fingerprints (along with the other associated data) which produce hits with the fingerprints entered in EURODAC by the other MSs of origin, an automated message will be sent to these latter MSs. This should ensure that MSs do actually delete the data to be deleted, so that no data are kept in the database longer than justified.
<i>To enable the Commission, the EDPS and national data protection authorities to effectively monitor the management of access to data in Eurodac by national authorities designated for the implementation of the Eurodac Regulation</i>	√√√	If, in their official notification, MS give details of the exact nature of the authority's national competences and of the relevant departments within the authority dealing with the application of the Eurodac Regulations, it will enable proper monitoring of MSs activities concerning EURODAC.
<b>Transposition feasibility</b>		
- Under existing treaty	√√√	No difficulties or risks are anticipated regarding the combination of the preferred suboptions.
- Under new treaty	√√√	No difficulties or risks are anticipated regarding the combination of the preferred suboptions.
Implementation costs	√√√	Cf. Annex 2.

### 7.1. Assessment and considerations of proportionality and EU added value

#### 7.1.1. Proportionality

Given the aim of a more efficient and consistent system for EURODAC, and the transnational nature of the problems identified in this IA, the combination of preferred suboptions offering solutions clearly justifies proportionate joint EU action in the framework of the Common European Asylum System (CEAS). Each suboption was assessed so as to represent an ideal proportion between practical value and efforts needed.

### 7.1.2. *Value added*

The preferred option ensures that the Regulation will be more consistently applied by Member States, while better providing for consistency with the EU *acquis* on asylum, in particular the Dublin Regulation.

## **8. MONITORING AND EVALUATION**

Statistics drawn up by the EURODAC CU will be used to monitor fulfilment of the operational objectives as described in 3.3.1. (avoiding ‘wrong hits’ and ‘missed hits’), 3.3.2. (ensuring that asylum applications of refugees are not processed) and 3.3.3. (ensuring deletion of data in circumstances foreseen by the current EURODAC Regulation). Concerning the first two points, relevant statistics are already produced every month, as a well-established practice. Concerning 3.3.3., the preferred solution consists of action by the CU, so monitoring of the automated provision of information will be equally unproblematic.

The fulfilment of operational objective 3.3.4. (enabling the Commission and EDPS to know who exactly is accessing data in each Member State) will be regularly monitored by the Commission.

Moreover, in order to monitor whether the revised Regulation is effectively enforced in the Member States, regular evaluation within the framework of the overall assessment of the Dublin system is suggested. Further regular EURODAC expert meetings will be organised to enhance the effects of the combination of preferred suboptions.

## **ANNEX 1: GLOSSARY ON ASYLUM**

### **Asylum**

Asylum is a form of protection given by a State on its territory based on the principle of ‘non-refoulement’ and internationally or nationally recognised refugee rights. It is granted to a person who is unable to seek protection in his/her country of citizenship and/or residence in particular for fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion.

### **Common European Asylum System**

Rules and principles at European Union level leading to a common asylum procedure and a uniform status, valid throughout the Union, for those granted asylum. The major aims and principles were agreed to in October 1999 at the European Council in Tampere (Finland) by the Heads of State or Government. The second phase in the establishment of the common European asylum system started with the adoption of The Hague programme in November 2004.

### **Non-refoulement**

The key principle of international refugee law, which requires that no State shall return a refugee in any manner to a country where his/her life or freedom may be endangered. The principle also encompasses non-rejection at the frontier. Its provision is contained in Article 33 of the 1951 Convention Relating to the Status of Refugees and constitutes the legal basis for States’ obligation to provide international protection to those in need of it. Article 33(1) reads as follows: ‘No Contracting State shall expel or return (refouler) a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion’. Article 3 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, in the light of the jurisprudence of the European Court of Human Rights and Article 3 of the UN Convention Against Torture and Other Cruel, Inhumane and Degrading Treatment or Punishment, are also considered as bases for ‘non-refoulement’ obligations.

### **Refugee**

A person who fulfils the requirements of Article 1(A) of the Geneva Convention. Article 1(A) defines a refugee as any person who, owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it.

### **Refugee status**

This is defined in the EU legislative instruments as the status granted by a Member State to a person who is a refugee and admitted as such to the territory of that Member State. In terms of the Geneva Convention, refugee status is defined as the status possessed by a person who fulfils the requirements of the refugee definition as laid down in the Convention.

### **Tampere European Council**

In October 1999 the Tampere European Council adopted a comprehensive approach to put into practice the new political framework established by the Treaty of Amsterdam in the area



of Justice and Home Affairs. The Council set ambitious objectives and deadlines for action in all relevant areas, including asylum and immigration, police and justice cooperation and the fight against crime.

### **The Hague programme**

The Tampere programme, adopted at the Tampere European Council in 1999, set the agenda for work in the area of Justice and Home Affairs for the period 1999–2004. Likewise, the European Council adopted in 2004 the Hague programme, which covers the period 2005–2010, and provides, among other goals, for the continuation of the efforts in establishing common European asylum and immigration policies.

## ANNEX 2: DESCRIPTION OF THE EURODAC SYSTEM

Created in the context of the Dublin Convention, Council Regulation 2725/2000/EC of 11 December 2000 for the establishment of 'EURODAC' (hereinafter: EURODAC Regulation) came into force on 15 December 2000 and the Community-wide information technology system for the comparison of the fingerprints of asylum seekers started operation on 15 January 2003.<sup>37</sup> Member States anticipated that identifying aliens who had already lodged an asylum application in another Member State would be difficult, if not impossible. When adopted in 2000, the Eurodac Regulation aimed at establishing a tool for the efficient application of the Dublin Convention. At the time of the adoption of the Eurodac Regulation, work had already started for the adoption of a Community instrument replacing the Dublin Convention, as the European Council agreed in Tampere in 1999.

After the entry into force of the Treaty of Amsterdam (having altered the legal basis and procedure for asylum policy), the form of a Regulation was chosen to integrate — on the basis of Title IV of the EC Treaty, in particular Article 63 — the provisions of the Dublin Convention into Community law, in view of the need to apply strictly defined and harmonised rules in all the Member States in relation to the storage, comparison and deletion of fingerprints.

The purpose of EURODAC is to facilitate the application of the Dublin Regulation, which is aimed at establishing a clear and workable mechanism for determining responsibility for asylum applications lodged in the EU Member States and in an area without controls at the internal borders. The Dublin system addresses two main issues:

- the phenomenon of **asylum shopping**, by preventing abuse of asylum procedures in the form of multiple applications for asylum submitted simultaneously or successively by the same person in several Member States;
- the need to guarantee effective access to the procedures for determining refugee status, ensure the rapid processing of asylum applications and thus avoid the phenomenon of **refugees in orbit**.<sup>38</sup>

The Eurodac Regulation provides for the implementation of a **Central Unit (CU)** managed by the European Commission containing an Automated Fingerprint Identification System (AFIS) which shall receive data and transmit 'hit — no hit' replies to the national Units (to the National Access Point [NAP] servers) in each Member State. The CU processes the fingerprints<sup>39</sup> and other data on individuals over the age of 14 as follows:

**Category 1** (hereinafter 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 (see below). This data will be *stored* for 10 years with the exception of one specific case (an individual who obtains the nationality of one of the Member States, in which case the data of the person concerned will be erased);

---

<sup>37</sup> Commission communication regarding the implementation of Council Regulation (EC) No 2725/2000 'Eurodac' (2003/C 5/03) OJ C 5 of 10.1.2003. The Central Unit of EURODAC began operating on 15 January 2003 with an empty database, meaning that only asylum applications lodged after this date can be stored in EURODAC.

<sup>38</sup> A situation where all MS claim *not* to be responsible for examining an asylum application.

<sup>39</sup> For those categories which are stored, the database contains the fingerprints, Member State of origin, sex, 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.

**Category 2** (hereinafter 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 2 years. However, they are deleted promptly when the individual receives a residence permit, leaves the territory of the Member State or obtains the nationality of one of them;

**Category 3:** While the storage of the two above is compulsory under the Regulation, MS 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 only are searched against the data of CAT1 stored in the central database.

*Before accepting any fingerprint data from the Member States, the Central Unit performs a quality check and is allowed to reject data and ask for that fingerprint data to be re-submitted.*

### **Member States**

Under the Regulation, the notion ‘Member States’ means all EU Member States, but also the states applying the Dublin *acquis*, i.e. Norway and Iceland.

### **Member State of origin**

According to Article 2(1) (c) the ‘Member State of origin’ is the Member State which transmits the fingerprints and other data to the Central Unit and (in case of CAT1 and CAT3 transactions) receives the results of the comparison.

### **Hit**

According to Article 2(1) (e), a ‘hit’ is a match or matches between fingerprint data recorded in the database and those transmitted by a Member State. NB under Article 4(6), Member States must immediately check the results of the comparison (‘human check’).

### **Erasure in advance**

According to Article 7 of the Regulation, data stored in the database as *CAT1* is erased (‘Advance data erasure’) before the elapse of the *default storage period of 10 years* if the person in question has acquired citizenship of a Member State. Similarly, according to Article 10, *CAT2* data is erased before the elapse of the applicable *2 years’ storage* period, in cases where the alien has been issued with a residence permit, has left the territory of the Member States or has acquired citizenship of a Member State. (CAT3 data is not stored in the database.)

### **DubliNet**

Article 22(2) of the Dublin Regulation provides for the creation of *a secure electronic transmission channel between the responsible authorities for transmitting the different types of requests* and ensuring that senders automatically receive electronic proof of delivery. DubliNet was created for this purpose.

The DubliNet system is a bilateral exchange of data between technical national access points (NAPs), sent over the s-TESTA network (Trans-European Services for Telematics between Administrations) which is a Generic Service of the Community IDA Programme (Interchange of Data between Administrations). This is an encrypted private network for public administrations, providing a secure telecommunications infrastructure based on IP (internet protocol).

The use of DubliNet is always compulsory except for the cases defined in Article 15(1) second subparagraph of Regulation 1560/2003/EC (Dublin Implementing Regulation).<sup>40</sup>

### Statistics:

EURODAC began its operations on 15 January 2003. On 31 December 2007, its central database contained 1 005 323 sets of fingerprints of asylum seekers and 80 923 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<sup>41</sup> and is currently capable of storing 1 600 000 ten print images. This implies that the EURODAC system has not yet reached the upper limit of its storage capacity.

The total of successful transactions sent to the CU in 2007 totalled 270 611, i.e. an average of 741 per day. The system is designed to process 3 750 transactions per day.<sup>42</sup>

- The number of transactions of data of asylum seekers<sup>43</sup> (CAT1, i.e. of those at least 14 years of age) was 197 284. 38 173 transactions were sent in as CAT2 (third-country nationals apprehended in connection with the irregular crossing of an external border).

---

<sup>40</sup> 'By way of derogation from the first subparagraph, correspondence between the departments responsible for carrying out transfers and competent departments in the requested Member State regarding the practical arrangements for transfers, time and place of arrival, particularly where the asylum seeker is under escort, may be transmitted by other means.'

<sup>41</sup> The Commission staff working document accompanying the Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, SEC(2007) 742 of 6 June 2007.

<sup>42</sup> See footnote 24.

<sup>43</sup> It should be noted that EURODAC data on asylum applications are not comparable with those produced by Eurostat, which are based on monthly statistical data returns from the Ministries of Justice and Interior. The main (methodological) reason for the difference is that Eurostat definitions include all asylum applicants of whatever age, with a distinction between first and repeat applications. In practice, Member States differ in terms of whether or not the dependants of asylum applicants are included in their asylum data. EURODAC contains fingerprints of asylum seekers from the age of 14 onwards.

### ANNEX 3: ADMINISTRATIVE COSTS (INCLUDING ONE-OFF INVESTMENT COSTS)

Preferred options: Problem 1 — Option C Problem 2 — Option Bb Problem 3 — Option C Problem 4 — Option A		Type of obligation	Description of required action(s)	Target group	Tariff (€ per hour)	Time (hour)	Price (per action or equip)	Freq (per year)	Nbr of entities	Total of actions	Total yearly recurring cost	Total one time cost
1	Problem 2 — Option Bb	Adapt IT system	Implementing changes to the EURODAC Central IT System	European Commission	Between EUR 59 000 and 110 000. 45 to 90 days of work for system supplier to implement the changes, between 200 and 300 hours for COM for definition of needs, procurement, testing and follow-up.					1		84 500
2	Problem 2 — Option Bb	Adapt IT system	Implementing changes to the MS IT Systems	EU27 + NO + IS	EUR 10 000 per country for changes to the local IT system by system supplier and 100 hours for each country to manage contract. EUR 10 000 estimate based on 10 to 20 working days for system supplier for each MS, estimated at EUR 500–1 000 per day. Contractor work includes analysis, implementation/installation and an elaborate test session with the EURODAC Central test system.					1		370 000
3	Problem 3 — Option C	Sending delete transaction to EURODAC	Consult local systems, delete if necessary and keep track of deletions	EU27 + NO + IS	26	0.30		200.00	29	29	45 240	
4	Problem 3 — Option C	Adapt IT system	Implementing changes to the EURODAC Central IT System	European Commission	Between EUR 66 000 and 95 000. 40 to 60 days of work for system supplier to implement the changes, between 350 and 450 hours for COM for definition of needs, procurement, testing and follow-up.					1		80 500
5	Problem 3 — Option C	Adapt IT system	Implementing changes to the MS IT Systems	EU27 + NO + IS	EUR 10 000 per country for changes to the local IT system by system supplier and 100 hours for each country to manage contract. EUR 10 000 estimate based on 10 to 20 working days for system supplier for each MS, estimated at EUR 500–1 000 per day. Contractor work includes analysis, implementation/installation and an elaborate test session with					1		370 000

					the EURODAC Central test system.				
						Total administrative costs (€)	45 240	950 240	
<p>The likely administrative burdens are only assessed for the preferred option(s).</p> <p>The cost estimates for changes to IT systems are based on past experiences with changes to the Central EURODAC IT system.</p> <p>To assess the number of deletions necessary, the following parameters were taken into account: number of deletions last 12 months – average number of hits – estimated growth of the number of deletions. The result was divided amongst EURODAC Members, giving a result of +/- 200 per MS. 0.3 hours is an estimate taking into account that these actions can be supported by automated tools. The cost per hour is based on a weighted average of the cost in EU27 administrations and the cost in NO&amp;IS and has been rounded.</p> <p>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).</p> <p>The 2005 figure has been rounded upwards, based on the assumption of economic growth and trends over the preceding years, and overheads of 10% have been added.</p> <p><a href="http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996_39140985&amp;_dad=portal&amp;_schema=PORTAL&amp;screen=detailref&amp;language=en&amp;product=Yearlies_new_population&amp;root=Yearlies_new_population/C/C4/C43/dbb10000">http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996_39140985&amp;_dad=portal&amp;_schema=PORTAL&amp;screen=detailref&amp;language=en&amp;product=Yearlies_new_population&amp;root=Yearlies_new_population/C/C4/C43/dbb10000</a></p> <p>Average employment costs in the European Commission in 2007, DG BUDG, note 24/11/2006, Adonis No 11216</p> <p>Average employment costs in the third/associated countries' public administrations: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (€32 in 2005).</p> <p>The 2005 figure has been rounded upwards, based on the assumption of economic growth and trends over the preceding years, and overheads of 10% have been added.</p> <p><a href="http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996_39140985&amp;_dad=portal&amp;_schema=PORTAL&amp;screen=detailref&amp;language=en&amp;product=Yearlies_new_population&amp;root=Yearlies_new_population/C/C4/C43/dbb10000">http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996_39140985&amp;_dad=portal&amp;_schema=PORTAL&amp;screen=detailref&amp;language=en&amp;product=Yearlies_new_population&amp;root=Yearlies_new_population/C/C4/C43/dbb10000</a></p>									