

EURODAC Supervision Coordination Group Report of the first coordinated inspection

Brussels, 17 July 2007

Secretariat of the Eurodac Supervision Coordination Group
EDPS,
Rue Wiertz, 60
B-1047 Brussels
e-mail edps@edps.europa.eu

Table of content

<i>I. Introduction</i>	3
<i>II. Background</i>	4
1. What is Eurodac?	4
2. Supervision of Eurodac	5
3. Coordinated inspection: a timely action	6
<i>III. Issues for inspection and methodology</i>	6
1. Issues	6
2. Method of inspection	7
<i>IV. Findings and evaluation</i>	8
1. Preliminary observations	8
2. Special searches	8
a. Legal framework	8
b. Reason for inspection	8
c. Findings	9
d. Evaluation	10
3. Use for other purposes	11
a. Legal framework	11
b. Reason for inspection	12
c. Findings	12
d. Evaluation	13
4. Quality of fingerprints	14
a. Legal framework	14
b. Reason for inspection	14
c. Findings	14
d. Evaluation	15
<i>V. Recommendations</i>	15

I. Introduction

This Report is the first one to be issued by the Eurodac Supervision Coordination Group, composed of representatives from the Data Protection Authority (DPA) of each of the participating States and the European Data Protection Supervisor. This report is the result of inspections carried out in a coordinated fashion by the DPAs supervising Eurodac. The scope of this type of coordinated supervision, exercised at national and European level, is likely to expand in the near future with the operation of new European databases, such as the second Schengen Information System (SIS II) and the Visa Information System (VIS). The Eurodac Supervision Coordination Group is pleased with the level of participation and welcomes the efforts invested in this project. The results of the inspections have provided valuable insights into issues arising in relation to the supervision of Eurodac, which can serve as a benchmark for future action.

At national level, this is the first time that the Eurodac system itself has been inspected thoroughly; the DPAs have developed their supervisory role towards Eurodac in a positive fashion through this action. The report considers different issues raised in the course of the operation of Eurodac and attempts to find a common approach to identify, analyse and where possible solve them.

In Chapter II, the report explains the background of this inspection (especially what Eurodac is, and how supervision is organised).

Chapter III details the issues which were selected and the method for inspection of these issues: special searches (type of queries in Eurodac intended for the exercise of the right of access of the individual), use of the data for other purposes, and technical fingerprint data quality.

In Chapter IV, the legal framework and reason for inspection are explained, followed by findings and evaluation, for each one of these three issues. A list of the Coordination Group's principal conclusions and recommendations is set out in Chapter V.

Terminology

For the purpose of this report, the following acronyms or terms must be understood as follows:

- Member State: any state to which the Dublin system applied when the decision to start national inspections was taken (autumn 2005). More specifically, the Member States participating to this inspection were all Member States of the EU except Denmark, plus Norway and Iceland.
- DPA: Data Protection Authority of one of the Member States
- Coordination meetings: meetings held by the European Data Protection Supervisor ("EDPS") and national DPAs (the "coordination group") in order to coordinate the supervision of Eurodac. Similarly, the "coordinated inspection" which is the object of the present report, is the inspection launched by the coordination group.
- Eurodac users: authorities in Member States which are in charge of the operation of Eurodac and/or have lawful access to Eurodac data.

II. Background

1. What is Eurodac?

Eurodac is an information system which was set up with the purpose of identifying the Member State responsible for an asylum application lodged within the European Union, in order to speed up the asylum procedure.¹ The Eurodac system enables Member States to identify asylum seekers and persons who have crossed an external frontier of the Community in an irregular manner. By comparing fingerprints, Member States can determine whether an asylum seeker or a foreign national, found illegally present within a Member State, has previously claimed asylum in another Member State. In addition, by being able to check if an applicant has already lodged a request for asylum in another Member State, "asylum shopping" in other Member States after being rejected in one can be avoided.

Created by a Regulation of the Council of Ministers, in December 2000², Eurodac has been operational since 15 January 2003 in all EU Member States (except Denmark), Norway and Iceland. In May 2004, ten new Member States joined the users group, followed by Denmark (on 1 April 2006), and in 2007, Romania and Bulgaria. Moreover, agreements have recently been signed with Switzerland and Liechtenstein in order to allow those countries to use the system, probably by around 2008.

In accordance with the Eurodac Regulation, all asylum applicants over the age of 14 have to have their fingerprints taken when they request asylum either within or outside of the EU. The fingerprints are then sent in digital format to Eurodac's Central Unit, which is hosted within the European Commission. The system compares the prints with others already stored in the database, thus enabling authorities to check if the applicant has already lodged an application in another Member State or if they entered the European Union without the necessary papers.

The Eurodac system is equipped with an Automated Fingerprint Identification System (AFIS) and an electronic data transmission application (provided by TESTA). AFIS receives data and transmits positive and negative replies to the National Access Points (NAPs) in the Member States. The system also allows Member States to exchange information about asylum seekers and illegal immigrants. Only national authorities dealing with asylum have access to the database.

Personal data processed by Eurodac falls into three categories: applicants for asylum of at least 14 years of age ("category 1"), aliens apprehended in connection with the irregular crossing of an external border ("category 2") and aliens found illegally present in a Member State ("category 3"). The following data are recorded:

- the Member State of origin,
- the fingerprint,
- the sex, and

¹ The implementation rules for Eurodac are set out in Council Regulation (EC) No 407/2002 of 28 February 2002.

² Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention (hereinafter, "the Eurodac Regulation").

- the reference number used by the Member State of origin.

In case of a hit, an additional exchange of data takes place through the DubliNet system. The Members States concerned can thus exchange personal data different from the Eurodac data: name, date of birth, nationality and photo, particulars of family members and in certain cases addresses.

In accordance with the Eurodac Regulation, the European Commission has to produce an annual report on the activities of the Central Unit responsible for operating the central database. Until now three reports have been submitted to the European Parliament and to the Council. The three annual reports underlined among others some issues related to data protection.

The Dublin and Eurodac Regulations also require the Commission to report to the European Parliament and to the Council on their application after three years of operation and to propose, where appropriate, the necessary amendments. This report should contain “an overall evaluation of Eurodac, examining results achieved against objectives and assessing the continuing validity of the underlying rationale as well as any implications for future operations” (Article 24(5) of the Eurodac Regulation).

This report, published on 6 June 2007, aims at assessing the application of both Regulations, from their respective entry into force until the end of 2005 (“the reference period”). It comprises two documents: a Report³, which presents the main findings and conclusions of the analysis carried out by the Commission services, and a Commission staff working document⁴, which contains the details of this analysis. This inspection report will refer to these documents where appropriate.

2. Supervision of Eurodac

Article 20 of the Dublin Convention provides that the supervision of Eurodac would initially be ensured by a provisional Joint Supervisory Authority, which was replaced by the EDPS at the beginning of 2004⁵. The EDPS is therefore now the competent authority for monitoring the activities of the Central Unit to ensure that the rights of data subjects are respected when their data is processed by Eurodac.

³ Report From the Commission to the European Parliament And the Council on the evaluation of the Dublin system, Brussels, 6.6.2007, COM(2007) 299 final. Hereinafter, “the Dublin Evaluation”.

⁴ Commission Staff Working Document, Accompanying document to the Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, Brussels, 6.6.2007 SEC(2007) 742. Hereinafter, “the Staff Working Document”.

⁵ Article 20, paragraph 11, lays down that: “The joint supervisory authority shall be disbanded upon the establishment of the independent supervisory body referred to in Article 286(2) of the Treaty. The independent supervisory body shall replace the joint supervisory authority and shall exercise all the powers conferred on it by virtue of the act under which that body is established”. In accordance with Article 20 (3) of the Eurodac Regulation, the EDPS is thus responsible for examining implementation problems in connection with the operation of Eurodac, for the examination of possible difficulties during checks by the national supervisory authorities and for drawing up recommendations for solving existing problems. Furthermore under Article 20 (4), the EDPS shall be actively supported by the national supervisory authorities.

At national level, each state participating in the Eurodac system has a supervisory authority, the DPA, to monitor the collection and use of data.

As already stated in the EDPS' first Annual Report 2004: "This (structure) means that the supervision must be exercised at both levels, in close cooperation." The EDPS therefore organised several cooperation meetings with the DPAs, where a common approach to supervision has been discussed.

The first meeting took place on 28 September 2005 and resulted in a plan of action for the future supervision of Eurodac. The participants decided to select a short-list of priority issues, which would be first investigated at national level, then brought together by the EDPS. Since then several meetings took place, where the progress of the national inspections was discussed.

This report is the result of the coordinated inspection and has been adopted during the coordination meeting of 28 June 2007. It aims at presenting the findings and recommendations with regard to the selected issues.

3. Coordinated inspection: a timely action

This report is especially timely, since it coincides with the publication by the Commission of the Dublin Evaluation. The results of the Dublin Evaluation will feed into the process of evaluation of EU policies on Justice, Freedom and Security, as detailed in the Commission Communication of 28 June 2006⁶. In this context, this report should represent a useful addition to this evaluation, with a specific emphasis on data protection issues. It may also lead to amendments to the Eurodac Regulation, where appropriate.

This report also represents a good opportunity to promote best practices, since Eurodac is a relatively young system, in that it has been in operation for 4 years (and even less in some countries). It is therefore still possible to correct some misunderstandings or misuses of the system before they become long-standing habits.

Finally, in the context of growing demands from the law enforcement authorities to use Eurodac data, as well as the plans to enhance interoperability of large-scale databases, one must realise that possible abuse of the database may have a much wider impact. It is therefore all the more necessary to avoid any misuse of the system.

III. Issues for inspection and methodology

1. Issues

In light *inter alia* of concerns expressed by the Commission, three main issues were selected:

1. special searches,
2. possible use for other purposes than foreseen in the Eurodac Regulation, and
3. the technical quality of data.

⁶ COM(2006) 332.

2. Method of inspection

An open questionnaire has been chosen as starting point. The problems were presented to the DPAs, but no precise questions were imposed for the national investigations. The questions asked were as follows:

1) Special searches

Special searches are legally limited to requests for access to personal data made by individuals (Article 18 of the Eurodac Regulation). However, the statistics provided by the Central Unit indicate that the number of special searches per country ranges from one special search query to more than 600 queries per year. Eleven countries performed less than 10 special searches per year. If the number of requests for access by individuals does not match the number of special searches actually performed, this discrepancy needs to be explained.

Moreover, DPAs were informed of the statistics concerning special searches, in order to get a good idea of the amplitude of the phenomenon in their respective country.

2) Use for other purposes

In accordance with the Eurodac Regulation, Eurodac may only be used in the framework of the asylum policy. In some countries, the national unit is operated by police forces, which raises some questions as to a strict use limitation of the system. In others, on the contrary, there seems to be a very strict limitation of use of category 3 searches about undocumented aliens, for fear of abuse by law enforcement or immigration services. It would be interesting to assess the situation in Member States, regarding the use of category 3 searches as well as access to the system by authorities other than asylum authorities.

3) Quality of data

From a more technical point of view, which system is used to collect and send the data? How is the performance assessed by your national authorities?

There have been several reasons to opt for an open questionnaire:

- The supervision of Eurodac is relatively new, and it was felt that this was not only an investigation into the issues raised above, but at the same time an opportunity to take stock of what has been achieved until now in Member States. In other words, this would enable the DPAs to become acquainted with the national Eurodac structure. Limiting or framing the questions too precisely could have prevented that.
- The overuse of special searches could have several reasons, none of which were known at the beginning of the national investigations. Therefore it was preferable to leave the question format very open in order not to influence responses and to keep an open mind as to possible unexpected answers.

This approach has proven useful in this context, since some of the results of national inspections were totally unexpected (see below, especially on the second question). At the same time, the drawback of this approach was that the resulting contributions were more heterogeneous and therefore also more difficult to compare.

IV. Findings and evaluation

1. Preliminary observations

Written answers⁷ to the questionnaire were received from Austria, Belgium, Czech Republic, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Lithuania, Luxemburg, Malta, the Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, United Kingdom.

Even though DPAs have carried out national inspections with varying intensity and the resulting inspection reports were therefore of various degree of detail, this can be considered as a good overall picture of the situation. Moreover, information gathered in the framework of this coordinated inspection could be complemented with information given by the Commission, either during the coordination meetings which have taken place since 2005, or in its annual or multi-annual reports on Eurodac.

2. Special searches

a. Legal framework

Article 18 of the Eurodac Regulation provides for the data subject's right to be granted information regarding the processing of his/her personal data by Eurodac. This is in line with current European data protection legislation (Article 12 of Directive 95/46/EC), which guarantees individuals the right of access to their personal data. The right of access to one's personal data is one of the most important principles of data protection and is closely linked to other rights, such as the right to have inaccurate data amended, deleted or blocked. These rights are also guaranteed by Article 18 of the Eurodac Regulation.

Upon receiving a request for access from a data subject, the Member State concerned sends the data of the requesting data subject to the Central Unit. As this is not a standard search as foreseen for applying the Dublin Regulation, this kind of search is classified as a "special search" (or a CAT 9 search, in Eurodac jargon). Article 18 foresees the use of a special search *solely* for the purpose of allowing data subjects to exercise their rights. The use of special searches for any other purpose than provided for in Article 18 is therefore unlawful.

b. Reason for inspection

As stated above, special searches are legally limited to requests for access to personal data made by the individuals concerned. The statistics provided by the Central Unit indicate that the number of special searches *per country* ranged in 2004 from one special search query to more than 600 queries. The numbers of such transactions in 2005 vary from zero to 781, while in 2006, they range from zero to 488. A great number of Member States performed less than 10 special searches a year, which means that an unusually high number of such queries were used by the same, small number of Member States.

⁷ Romania also sent a written contribution although it was not a Eurodac Member State during the reference period of the inspection. It has been taken into account for information, but has not been integrated into the "findings" and "evaluation" parts of this report.

The main concern is the following: if the number of requests for access by individuals does not match the number of special searches actually performed, this discrepancy needs to be explained. It is indeed hard to believe that some Member States would deal with hundreds of requests for access a year, while other Member States would have none.

Since 2004, the Commission services have expressed concerns about the surprisingly high number of “special searches”. The Commission services have alerted the EDPS and directly contacted some Member States of particular concern.

Some national authorities have already informally explained to the Commission the reasons for such a frequent use of this special category of searches. Namely, such transactions which do not lead to storage of data, would be used in cases where the responsible authorities have lost track of a previous transaction and therefore lost the fingerprints sent back by the Eurodac Central Unit when a hit occurred.

c. Findings

The main results as given by the respondent Member States could be summarized as follows, over the period from January 2005 to June 2007 (period of reference):

Full compliance with the Regulation (because no special searches at all were performed or because they were explained by a data subject’s right of access)

4 Member States never used any special search; in 2 of these Member States, although the special searches have never been used, the DPA has already instructed the responsible bodies of the penalties in case of misuse of the Eurodac System and announced its intention to monitor them anyway.

It is striking to see that in only 2 Member States, the DPA has been informed that the special searches actually performed were used lawfully, i.e. for the right of access.

In 2 other ones, special searches have been used by mistake in the past (before 2006), but staff have been instructed to use them only for the right of access. There has been no special search ever since, and one can assume that full compliance is now ensured.

That would mean that in 8 Member States (a third of the Member States participating in the coordinated inspection), the Eurodac Regulation was fully complied with.

Wrong handling

2 Member States reported that the special searches were used because of a manual error of operators. In both cases, they concerned minor numbers of queries: 2 and 3 respectively. These errors were traceable and justified one year after they were carried out.

In 2 other Member States, special searches (performed in small numbers) were not justified. The Eurodac authorities assumed they were due to sporadic errors. However, the responsible authorities were unable to trace these operations.

Training and testing

In 6 Member states, including some frequent users of special searches, this category of query was used for training and testing purposes. In all of them, it seems that this mistake has been committed in good faith, by responsible bodies which were unaware of other means of testing the system. The Commission has informed the DPAs during the meeting of 28 June 2006 of the possibility of using the Business Continuity System (BCS) for these purposes⁸. The information has been passed on by DPAs to their national responsible authorities with the result that these operations have now almost ceased entirely in these Member States.

Misconceptions about the use of special searches

In 3 Member States, it appears that staff has been incorrectly trained as regards special searches and uses them either as CAT3 searches or in order to check the data already fed into the system previously, when there is a suspicion that data need to be corrected. In these cases, staff has now been instructed of the right use of special searches.

In 1 Member State, data have been consulted on behalf of another state which was not a member of the Eurodac system at the time. The Commission has already addressed this error which has been promptly corrected.

Unexplained

In 2 Member States, no explanation at all has been received in the course of this inspection.

d. Evaluation

The evaluation leads to a somewhat paradoxical conclusion: there is cause for satisfaction because special searches have been conducted mostly by mistake, and do not involve a misuse of the system (i). On the other hand, it is worrying to see that so few special searches have been conducted for the reason they were intended for: the right of access of the individual (ii). This scant use of the right of access by the individuals involved may be due to a lack of awareness, which itself could indicate that the information to the individuals concerned is not adequate.

(i) One positive outcome of this inspection is that, apparently, all special searches have been performed in good faith, by mistake. The mistakes were mainly due either to a wrong handling of the equipment itself, or to lack of information about the possibility of testing the system and training staff using the BCS. The need for training and testing explains the biggest number of special searches.

That being said, even though it is reassuring to see that no deliberate abuse was involved, this situation naturally triggers questions as to the adequacy of the training of staff on the one hand, and the level of information provided to the Eurodac authorities themselves on

⁸ The Commission also reminds in the Staff Working Document, p.37, that “the Business Continuity System has also testing capabilities to allow Member States or Accession Countries to test any new solutions being implemented by a National Access Point and therefore prevent issues arising with the “live” Central Unit”.

the other. There is certainly room for improvement in this respect. Another slightly worrying aspect is that in many cases, Eurodac authorities were unable or unwilling to justify even very few special searches when it was requested by their DPA. This should also be improved in the future. Finally, it should be noted that in some Member States, the authorities complained that there was no way of correcting manual errors: once the CAT9 search had been chosen, even though the operator immediately realises his mistake, he cannot correct this error in the system.

Another very positive element is that, even before conclusions could be officially drawn from the coordinated inspections, the fact that investigations were undertaken by the DPAs has had a noticeable impact on the number of special searches performed overall. They have dropped by more than 50% between 2005 and 2006, and at least by another 50% between 2006 and June 2007. In most Member States, they have dropped to a point where it can be considered that they are probably due to isolated mistakes or confusions. The situation remains worrying in one Member State (although even there, a noticeable decrease in the use of special searches has occurred in recent months).

This is certainly due to a large extent to the fact that DPAs have taken action against their national authorities. It should be noted that the length of the coordinated inspection was in a way a positive factor: DPAs were able to compare information concerning their respective Member State to information provided by others.

Moreover, some difficulties only became evident after the completion of a few inspections, and allowed the Commission to give the necessary information to remedy these difficulties. More specifically, for instance, when it became apparent that many Member States used the special searches for training and testing purposes, it allowed the Commission to clarify the role of the Business Continuity System in this regard. This, in turn, enabled DPAs to pass on this message to their national Eurodac authorities. Consequently, in the course of the inspection itself, remedial action has already been taken.

(ii) However, as mentioned before, the fact that the wrong use of special searches is decreasing does not lead to an unmitigated satisfaction. It is worrying to see that the right of access has been used so scarcely. The special searches are an indicator of this, since there is no other way to access the data in Eurodac. According to the information received in the course of this inspection, the right of access has been requested in two Member States only. This element alone shows that asylum seekers are probably not sufficiently aware of their right to obtain access to and correct their data.

Therefore, Member States should certainly not tackle exclusively the issue of inappropriate use of special searches, but also endeavour to increase the lawful application of Art.18.

The coordination group sees this as an important issue and intends to deal with it in more depth in the future.

3. Use for other purposes

a. Legal framework

Article 1 (1) of the Eurodac Regulation, clearly stipulates the purpose of Eurodac: "to assist in determining which Member State is to be responsible pursuant to the Dublin

Convention for examining an application for asylum lodged in a Member State, and otherwise to facilitate the application of the Dublin Convention ...". Eurodac may therefore only be used in the framework of the asylum policy.

Furthermore, Recital 15 states that Directive 95/46/EC applies to the processing of data by the Member States within the framework of the Eurodac system. Since Article 6 (1b) provides that data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes", the above provisions of the Eurodac Regulation are in line with this legislation.

In accordance with Articles 13 (2) and 14 of the Eurodac Regulation, Member States have to ensure that any use of the data in the Central database which is not in line with the purpose of Eurodac shall be subject to appropriate penalties.⁹

b. Reason for inspection

In accordance with the Eurodac Regulation, Eurodac may only be used in the framework of the asylum policy. In some Member States, the national unit is operated by police forces, which may raise some questions as to a strict use limitation of the system. In others, there seems to be a very strict limitation of the use of category 3 searches about undocumented aliens, for fear of abuse by law enforcement or immigration services.

In view of the diversity of national systems in this regard, it has been considered interesting to see how compliance with the principle of purpose limitation was ensured. The situation in Member States regarding the use of CAT 3 searches as well as access to the system by authorities other than asylum authorities was to be assessed.

c. Findings

The structure of the management of Eurodac varies widely from Member State to Member State, with regard to the nature and/or number of authorities in charge (Eurodac authorities). In this respect, it should be borne in mind that the Eurodac Regulation defines the purposes for which data can be processed but does not impose a particular structure or nature of the authority in charge.

Nature of these authorities

In some Member States, Eurodac is entirely operated by the national police services, in others, entirely by asylum or immigration authorities. In most Member States, though, responsibilities are shared between different authorities with different competences (see below).

The fact that Eurodac is in many Member States partly or entirely operated by police forces did not lead to the detection of any abuse by the inspecting DPAs, although this would be monitored further in some Member States. In one Member State, though, it has been noted that the list of authorities having access to results of CAT3 comparisons is very long and includes authorities in principle not involved in asylum procedures (such as

⁹ Recital 19 and Article 25 of the Eurodac Regulation. See also Commission Staff Working Paper on the Dublin Evaluation, p 45.

the tax authority, for instance). In another Member State, Eurodac can be used, on the request of a magistrate, to identify corpses. In both cases, the DPAs will further investigate these questions.

However, apart from these situations, the distinction of purposes seems clear; the DPAs did not mention receiving any complaint (from data subjects or interested NGOs, for instance) about this.

Some Member States have even implemented systems or routines whereby it is ensured that no unwarranted access by the police is possible at all, especially when it concerns CAT3 searches. In one of these Member States, the police authority requesting the identification of an undocumented alien must justify for each case why there are reasons to believe that the alien in question could be reported in Eurodac. This ensures that Eurodac is not used as a routine identification tool. In another Member State, the Police federal office filters the requests for CAT3 searches to ensure that they are identified as Eurodac cases, and keeps trace of all consultations of the database, for evaluation purposes. In a third one, Eurodac data can be accessed only by staff in charge of asylum procedures, with a specific clearance, thereby ensuring that only Eurodac staff can access these data.

Number of authorities with Eurodac responsibilities

One of the most striking (and unexpected) outcomes of the inspection was that, in several Member States, the DPAs have had a very difficult job in identifying all authorities with Eurodac-related responsibilities, let alone to identify which one was the actual data controller. In several cases, the police authorities collect data while asylum authorities process them further (sending them to the central unit and pass on the result of the comparison to the requesting authority).

While splitting of responsibilities is in itself perfectly acceptable, this led in some Member States to a situation where none of the authorities wanted to acknowledge its responsibilities for any problem that might arise in the operation of Eurodac. It even seems that, in two Member States, the Eurodac users were not even known to one another, nor was their exact role in the processing.

d. Evaluation

There does not seem to be a major problem concerning the respect of the purpose limitation principle or access by unauthorised authorities to Eurodac. The fact that no complaint has been received concerning this by any DPA may also confirm this assessment (however, we must be cautious in drawing this conclusion, as it may be due to a lack of awareness of Eurodac rights among asylum seekers).

However, even in this situation, it is advisable not to rely entirely on spontaneous compliance by staff of Eurodac authorities, but to put in place routines or methods which would ensure that compliance is ensured. An exchange of best practices specifically in this area could be envisaged.

As to the shared responsibilities, it should be noted that, even though the principle in itself is not problematic, its application is. The situation should not arise where the main

data controller cannot be identified. In the cases of Member States with the most intricate set-up, the DPAs have taken action to request that the identity of the data controller is communicated to them.

4. Quality of fingerprints

a. Legal framework

Under Article 13 of the Eurodac Regulation, Member States are responsible for ensuring that fingerprints are taken lawfully, that they are lawfully transmitted, accurate and up to date, lawfully recorded, stored, corrected and erased. Moreover, data quality is also a basic requirement of Directive 95/46/EC, which is applicable to Eurodac.

b. Reason for inspection

The Commission has previously expressed concerns about data quality on several occasions. Currently, 6% of data is rejected due to low quality; this has been the case in the last years as well. Hence there is concern that not enough is being done to improve the quality of data.

The Commission has suggested improving the quality of data by organising specific training, local quality checks, and the use of state of the art equipment, such as live scanners.

Within this context, it has been considered useful to find out what equipment Member States were currently using, what experience they had and if they have encountered any problems. Furthermore Member States which have very low rejection rates could share their knowledge with others to contribute to having consistent quality standards throughout Eurodac and the Dublin system.¹⁰

c. Findings

The states which participated in the national inspection have in general expressed satisfaction with the quality of data. However, there was also a general assessment that optic scanners, such as live scan, perform much better than ink-fingerprinting. Two Member States also made the point that in the case of optic scanners, any deficiency in quality is immediately established. Another Member State noted a higher rejection rate for ink fingerprint cards than for electronic cards.

One Member State also pointed out that fast searches (2 fingers), such as those which are performed in emergency cases, were found to have a higher rejection rate. The quality of fast searches is to be improved in the long term by requiring the prints of four fingers to be taken.

Apart from these issues regarding data collection, some Member States identified specific technical problems with the actual system. For example, in one case the high rejection

¹⁰ On this point, see also Commission Staff Working Document, accompanying document to the Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, 6 June 2007, p. 38.

rate was traced back to the quality filter at the Central Unit. Perhaps this could be improved through human intervention.

A significant number of Member States have also emphasised the importance of training, by, for example compiling manuals and organising training programmes for staff concerning asylum procedures. In one Member State, more resources are currently being invested in training than in technical resources.

One Member State mentioned a high number of cases of “impossibility to enrol”, i.e. where the individual has no usable fingerprints, because of disabilities, age, mutilation (apparently self-inflicted in more and more cases) or other reasons. This is a phenomenon of growing relevance in a system such as Eurodac.

d. Evaluation

Two elements are found in nearly all national reports:

- The quality of equipment is important: obviously, Member States still using ink fingerprinting would be keen to have live scans instead. This is not really a surprise, and is consistent with the Commission’s findings in this respect. However, there are issues of cost involved, which explains the difficulties encountered in many Member States.
- Even where the equipment is of high enough quality and precision, training is also a crucial element. The purchase of good equipment must be accompanied by adequate training of staff; otherwise even the best equipment cannot provide accurate results. The Commission rightly emphasises this in its Dublin Evaluation.

Finally, the phenomenon of impossibility to enrol should be analysed further, since it is of growing relevance for the issue of data quality.

V. Recommendations

In view of the findings of the coordinated inspection, the Eurodac Supervision Coordination Group recommends the following:

Special searches

- National Eurodac authorities must at all times be able to account for every special search, whatever its reason. The DPAs will monitor at regular intervals that this is the case.
- If Eurodac authorities find that they have to use the special searches because of lacunae in the existing system (impossibility to correct manual errors, for instance), they should report this to their DPA as well as to the Commission, in order to enable the devising of structural solutions.
- The Commission must ensure that the authorities in Member States are adequately informed about Eurodac, including the possibility of using the Business Continuity System for training and testing purposes.
- National Eurodac authorities must ensure that their staff are adequately trained, in particular about the authorised use of the special searches.

- The Member States should promote and encourage the exercise by the persons concerned of their right of access to data relating to them in Eurodac. In particular, Member States could do so by ensuring that adequate information is provided to the data subject, giving consideration to the specific needs of this category of data subjects (e.g. in terms of language).

Use for other purposes

- Eurodac authorities must identify clearly the responsibilities of the different services using Eurodac in their respective Member States. In particular, a data controller (or joint controllers where appropriate) must be identified and reported to the national DPA. The number of authorities having access to the results of Eurodac searches must be limited, as appropriate.
- Where different authorities share the responsibility of the data processing (from collection to comparison of the data in Eurodac), it should be ensured that these different responsibilities are organised in such a way that lawful processing of data is guaranteed and that data are updated and corrected when necessary. Similarly, security of the data must be ensured at all stages of the processing.
- Eurodac authorities should develop written and formal procedures to ensure that access to Eurodac data is limited to the purposes of the Eurodac Regulation. In particular, request of CAT3 searches should be documented in such a way that they are used in strict compliance with the Eurodac Regulation.
- Generally speaking, Eurodac authorities must guarantee the transparency of their activities vis-à-vis their national supervisory authorities. They should provide DPAs all information relevant for their tasks even proactively when appropriate.

Quality of fingerprints

- Member States should take every step to ensure a better quality of fingerprints than now sometimes available. The use of live scans rather than ink fingerprinting is preferable wherever possible. Eurodac authorities should invest in adequate training for their staff. The Commission has committed to increase its effort in training as well.
- The Eurodac authorities should share with the Commission the specific difficulties they identify with regard to the quality of data, in order to come to common solutions.