Coordinated Supervision of Eurodac

Activity Report 2012-2013

Brussels, May 2014

Secretariat of the Eurodac Supervision Coordination Group
European Data Protection Supervisor
Rue Wiertz 60
B-1047 Brussels
email: eurodac@edps.europa.eu

Table of Contents

1. Introduction

Eurodac is an information system established for the comparison of fingerprints of asylum applicants and irregular immigrants. It facilitates the application of the Dublin Regulation[1] which aims at determining the State responsible for examining the asylum application.[2] Eurodac has been created by Council Regulation (EC) No 2725/2000 of 11 December 2000[3] as completed by Council Regulation (EC) No 407/2002 of 28 February 2002.[4] The system has been operational since 15 January 2003 and is currently used by the 28 EU Member States as well as Iceland, Liechtenstein, Norway and Switzerland.[5]

As established in the Eurodac regulation, data protection supervision of the Eurodac system is carried out at national level by the national supervisory authorities (data protection authorities, hereafter "DPAs"), while for the central (EU) level, the European Data Protection Supervisor (EDPS) is competent. The coordination between the two levels is ensured by the Eurodac Supervision Coordination Group (hereafter "the Group"), which is composed by representatives of the DPAs and the EDPS. In 2012-2013, this Group continued to be chaired by Mr Peter Hustinx (EDPS), while the Vice-Chair was Ms Elisabeth Wallin (Swedish DPA). The present document reports on the activities of the Group for this period.

The need for thorough data protection supervision of Eurodac is evident when considering the category of persons affected by the Eurodac system: asylum seekers and (to a lesser extent) irregular immigrants. This need is also reinforced by the evolution of policies in the area of freedom, security and justice in recent years. Asylum policies need to be better coordinated, and, as a result, so does the protection of the rights and freedoms of asylum seekers.

Data protection is also a key factor for the success of the operation of Eurodac, and consequently for the proper functioning of the Dublin system. Elements such as data security, quality of data and lawfulness of consultation of Eurodac data all contribute to the smooth functioning of the system.

---

[1] Regulation (EC) N° 343/2003 of 18 February 2003 and Commission Regulation (EC) N° 1560/2003 of 2 September 2003, OJ L 222, 05/09/2003 P. 3 - 23. These two instruments are sometimes called "Dublin II".

[2] 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 irregularly present within a Member State has previously claimed asylum in another Member State.

[3] 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 "Eurodac Regulation", OJ L 316 , 15/12/2000 P. 1 - 10.

[4] Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 62, 5/3/2002, P. 1–5.

[5] When Eurodac was established, it was used in the then EU-15 Member States (except Denmark), as well as in Norway and Iceland. Since then, the system has been joined by the ten new Member States following the 2004 enlargement, by Denmark (2006), Bulgaria and Romania following the 2007 enlargement, as well as Switzerland (2008). Finally, a protocol between the Union, Switzerland and Liechtenstein, allowing the latter to join the system, entered into force on 1 April 2011.

Section 2 of this report clarifies the legal environment including the challenges posed by the evolution of the legal framework. In the period covered by this report, the discussions on a reform of the Eurodac Regulation continued and in 2013 a new set of rules was adopted by the EU legislator. The new Eurodac Regulation has been published in the Official Journal on 26 June 2013[6] and shall apply from 20 July 2015.

Section 3 summarises the proceedings at the four coordination supervision meetings which took place during the reporting period.

Achievements are the subject of section 4: during the last two years, the Group kept up its good work from the previous reporting period, conducting an inspection on unreadable fingerprints and adopting a common format for national inspections.

Section 5 concludes the report by giving a brief general overview of activities to come in the next reporting period to the extent they can already be anticipated.

2. Legal framework: Revision of the Eurodac Regulation

There are several new topics that become prominent under the new rules. The Eurodac Regulation has a set of different data protection rules applying either for the purpose of determining the Member State responsible for examining an application for international protection or for law enforcement purposes.

The most relevant change in terms of data protection implications is the ***access of law enforcement authorities*** (including Europol) to Eurodac data. The authorities having access, the conditions for access and its modalities, how data is transferred to third countries are subjects of interest to the Group. There are also questions concerning the information of the data subject, follow up on special searches or marking of data that will have to be viewed in the new framework. In the light of the new Eurodac Regulation, which provides that the EDPS shall ensure that an audit following international standards is performed on the central unit at least every 3 years, national DPAs could also follow the same approach by using a common format linked to the obligation to perform audits in other large IT systems (such as VIS).

Eurodac data ***shall not be transferred*** or made available to any third country, international organisation or private entity established in or outside the Union. This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Article 2(b) of Framework Decision 2008/977/JHA. Personal data which originated in a Member State and are exchanged between Member States following a hit obtained for law enforcement purposes shall not be transferred to third countries if there is a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights.

[6] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 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 and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ 29.6.2013, L 180/1.

The ***updates on the eu-Lisa and the Commission action*** should continue to be for the Group attention. The new Regulation defines the relation and division of competences between the Commission and eu-Lisa and their objectives and measures that have an impact also on national systems should be discussed within the Group.

The new Regulation will likely have an impact on the follow up of ***special searches*** in that it provides for a mandatory logging of all requests for access. It will be easier to compare numbers (special searches on the one hand, requests for access on the other hand) and to take action on that basis. This will help to tackle the main concern which is to check if the number of requests for access by individuals does match the number of special searches actually performed.

Marking of data**:** references to the "blocking" of data were changed to the "marking" of data concerning recognised beneficiaries of international protection. Under the original Regulation, the data of persons granted international protection remained on the Eurodac system but were blocked. As such, the Eurodac system recorded when there were hits concerning the fingerprints of recognised beneficiaries of international protection, but Member States were not informed of these hits. The new Regulation was designed to "mark" these data instead of blocking, in order to inform the Member States if there is a hit for a marked data subject. This is to inform Member States if an existing beneficiary of international protection attempts to put in a fresh claim for asylum.

Information to data subjects and to professionals. In the new Regulation, the wording on the leaflet has been enhanced to ensure that it is simple and written in a language the applicant can understand.

The new Regulation confirmed the approach to ***coordinated supervision*** – the current model of coordination between national DPAs and the EDPS, each acting within their respective competences, therefore remains unchanged.

3. Organisation of coordinated supervision

3.1. Main principles

As in previous years, the cooperation took the form of meetings held on a regular basis with all DPAs in charge of supervising Eurodac at national level and the EDPS, acting together as Eurodac Supervision Coordination Group (SCG). The main purpose of these meetings was to discuss common problems related to supervision and find common solutions or approaches whenever possible. According to Article 5 of the Group's rules of procedure, these meetings shall take place at least once a year. In practice, two meetings are held per year. The Commission is also invited to parts of the meetings in order to update the Group on new developments regarding Eurodac.

3.2. The supervision coordination meetings

In the period 2012-2013 four supervision coordination meetings have taken place on the following dates:

- 24 May 2012;
- 21 November 2012;
- 12 April 2013;
- 16 October 2013.

The meetings were held in Brussels, usually back to back with meetings of the VIS SCG (see below) in the EDPS premises.

Typically, the first part of the meeting is devoted to a presentation by the European Commission services involved in the management of Eurodac, either on technical or legal aspects. This helps to ensure that the Group is always up-to-date on recent developments in order to ensure effective supervision. The second part is devoted to discussion between DPAs on issues that are in need of checking at national level or on new developments of interest for Eurodac supervisors.

The following paragraphs quickly recapitulate the topics discussed and actions taken at the different meetings. A more detailed description of selected actions will follow in section 4 of this report.

Meeting on 24 May 2012

The Group took stock of the latest legislative developments on Eurodac and included representatives of the UNHCR and the Commission in discussions on the access of law enforcement authorities to the system. The coordinated security audit questionnaire, which was close to completion, was discussed with the aim of providing national data protection authorities a common framework for security audit methodology. A state of play on the "failure to enrol" exercise was also presented. "Failure to enrol" refers to applicants for asylum whose fingerprints are not readable for various reasons. The aim of this exercise was to explore and share the differences in dealing with "failure to enrol" in Member States with recommendations of best practice. Along with adopting its activity report for 2010 and 2011, the Group took note of the latest developments on the Visa Information System (VIS) with a view to officially launching the VIS Supervision Coordination Group before the end of 2012.

Meeting on 21 November 2012

The Group took stock of the latest legislative developments in the Eurodac Recast, the move of the management of the system to a new IT Agency foreseen for the end of 2012 and the follow up of the EDPS inspection of February 2012. The Group also discussed the results of an on-going exercise "failure to enrol" and adopted a common methodology for security audits (see point 4.1).

Meeting on 12 April 2013

At the meeting, the Group took stock of the latest legislative developments in the Eurodac Recast, where discussions were approaching conclusion, and discussed the transfer of operations to the IT agency, eu-LISA, in Strasbourg. The Group also adopted under written procedure the report on unreadable fingerprints (see point 4.2).

Meeting on 16 October 2013

The Commission and eu-Lisa representatives provided the Eurodac SCG with the usual update on recent developments. The Group discussed the results of a questionnaire sent by the Commission to the Member States to check the application

of current Eurodac rules, including on issues such as the number of transactions of each Member State, the quality of data or the advance erasure of data.

The Group decided to stay in touch with the Commission services in order to exchange relevant information on these aspects, and to allow national DPAs to give follow up where necessary. Eu–Lisa representatives announced that they took over the operational management of Eurodac from the Commission and presented the current plans of transferring the Eurodac system from Luxembourg to Strasbourg.

Based on a Note prepared by the Eurodac SCG Secretariat, the Group had a first discussion on main data protection implications of the Eurodac Recast which will be applied in July 2015. The members of the Group shared relevant information about national inspections on the Eurodac system in different Member States and other recent developments such as the increase of asylum requests from Syrian refugees.

4. 2012-2013: Issues discussed and achievements

4.1. Security audit methodology

According to the Eurodac Work Programme for 2010-2011 the development of an audit framework has been foreseen as one of the main exercises to be started and carried out by the Group. Though the audit methodology may vary from country to country, the selected standards should be consistently high. In view of these elements, a methodology for developing a framework - at least on main lines - has been agreed to be developed by the Group.

A security sub-group consisting of the EDPS and DPAs from Spain, Greece and U.K has been established. Aim of the sub-group was to prepare a common methodology for inspections at the national EURODAC access points that could be applied by all Member States. The EDPS, Greece, Spain and the UK worked on the draft, and on the basis of the draft questionnaire, investigations have already taken place in some Member States. The aim of the questionnaire adopted by the Group and distributed to all DPAs at the end of 2012 is to help national inspections, but it is not meant to be prescriptive. The questionnaire is designed to cover data protection and security concerns.

The methodology was to prepare data protection and security questions with regard to technology and compliance with legal rules. The questionnaire was mapped on to the Eurodac regulation (both the regulation currently in force and the last proposal for a recast).

The questionnaire, presented as "Standardised inspection plan for EURODAC NAP", covers the formal and informal procedures in place to ensure the secure and authorized collection, storage, handling, transmission and any other processing of EURODAC data within, between, to and from the National Access Points ('NAPs') and the Central Unit. This includes an evidence column for supporting documents. The information gathered will help to understand and appreciate national characteristics in this regard, eliminate perceived security risks, facilitate constructive dialogue between the Member States, establish a common best practice and identify areas for improvement, legal and otherwise.

4.2. Unreadable Fingerprints Report

The collection and further processing of fingerprints occupy a central place in the Eurodac system. The processing of such biometric data poses specific challenges and creates risks which have to be addressed. In this context, the problem of 'failure to enrol' —the situation in which persons find themselves if for some reason, their fingerprints are not usable— is one of the main risks.

The questionnaire adopted in 2011 pursued two aims:

1. To receive an overview of the practices for dealing with unreadable fingerprints;
2. To identify best practices and possible improvements.

To this end, it was divided into two sections, five questions for the competent authorities, aiming to find out what procedures for dealing with unreadable fingerprints are in force and three questions for data protection authorities (DPAs), focusing on legal aspects and their assessment of the situation.

Based on the analysis of the replies received, the report included several recommendations to competent authorities in the Member States to establish clear and binding procedures. These recommendations should allow asylum seekers to benefit from harmonised practices throughout the EU (avoiding possible discrimination). The procedures should clarify that unreadable fingerprints are not to be used per se against applicants, but that any adverse consequences for applicants need to be justified by sufficient evidence.

One of the recommendations for best practice is to oblige competent authorities in the Member States to retake fingerprints after a given time (for example two weeks) in order to allow the ridges to regenerate and, if possible, involve a specialist forensic or technical officer at the procedure. To decrease the administrative burden and related stress, a common minimum time for retaking fingerprints should be established. This will benefit asylum seekers as well as the national authorities. It should also be decided whether the applicant, when detained, is to be informed of the fingerprint retaking. Asylum seekers should also be assured of the right to lodge a complaint against the relevant national authorities or even national data protection supervisory authorities.

5. What to expect in 2014

The Work Programme for 2013-2014 concentrates on the need to supervise the transition to the EURODAC rules that will come into effect in June 2015 according to the new EURODAC provisions.

Planned activities include the following:

- Analysing the new Eurodac Regulation and its implications for data protection supervision (notably including access for law enforcement authorities);
- Improving consistency in inspections/audits;
- Continuing work on the adopted common framework for inspections.