P6_TA(2009)0378

Establishment of 'Eurodac' for the comparison of fingerprints (recast) ***I

European Parliament legislative resolution of 7 May 2009 on 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] (recast) (COM(2008)0825 – C6-0475/2008 – 2008/0242(COD))

(Codecision procedure – recast)

The European Parliament,

– having regard to the Commission proposal to the European Parliament and the Council (COM(2008)0825),

– having regard to Article 251(2) and Article 63(1)(a) of the EC Treaty, pursuant to which the Commission submitted the proposal to Parliament (C6-0475/2008),

– having regard to the Interinstitutional Agreement of 28 November 2001 on a more structured use of the recasting technique for legal acts[1],

– having regard to the letter of 3 April 2009 from the Committee on Legal Affairs to the Committee on Civil Liberties, Justice and Home Affairs in accordance with Rule 80a(3) of its Rules of Procedure,

– having regard to Rules 80a and 51 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A6-0283/2009),

A. whereas, according to the Consultative Working Party of the legal services of the European Parliament, the Council and the Commission, the proposal in question does not include any substantive amendments other than those identified as such in the proposal and whereas, as regards the codification of the unchanged provisions of the earlier acts together with those amendments, the proposal contains a straightforward codification of the existing texts, without any change in their substance;

1. Approves the Commission proposal as adapted to the recommendations of the Consultative Working Party of the legal services of the European Parliament, the

---

[1] OJ C 77, 28.3.2002, p. 1.

Council and the Commission and as amended below;

2. Calls on the Commission to refer the matter to Parliament again if it intends to amend the proposal substantially or replace it with another text;

3. Instructs its President to forward its position to the Council and the Commission.

P6_TC1-COD(2008)0242

Position of the European Parliament adopted at first reading on 7 May 2009 with a view to the adoption of Regulation (EC) No .../2009 of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ***(recast)***

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 63*, first paragraph,* point (1)(a) thereof,

Having regard to the proposal from the Commission ‖,

Acting in accordance with the procedure laid down in Article 251 of the Treaty[1],

Whereas

(1) A number of substantive changes are to be made to 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[2] and 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[3]. In the interest of clarity, those Regulations should be recast.

(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who ▌ legitimately seek ***international*** protection in the Community.

(3) The first phase in the creation of a Common European Asylum System that should lead, in the longer term, to a common procedure and a uniform status valid throughout the Union for those granted asylum, has now been *completed*. The European Council of 4 November 2004 adopted the Hague Programme, which sets the objectives to be implemented in the area of freedom, security and justice in the period 2005-2010. In this respect, *the* Hague Programme invited the ‖ Commission to conclude the evaluation of the first phase legal instruments and to submit the second-phase instruments and measures to the Council and the European Parliament with a view to their adoption before 2010.

---

1 *Position of the European Parliament of 7 May 2009*.

2 OJ L 316, 15.12.2000, p. 1.

3 OJ L 62, 5.3.2002, p. 1.

(4) For the purposes of applying ‖ Regulation (EC) No […/…] *of the European Parliament and of the Council of ...* 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[1], it is necessary to establish the identity of applicants for international protection and of persons apprehended in connection with the ***irregular*** crossing of the external borders of the Community. It is also desirable, in order to ***effectively*** apply ‖ 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], and in particular points (b) and (d) of Article 18(1) thereof, to allow each Member State to check whether a third-country national or stateless person found illegally present on its territory has applied for international protection in another Member State.

(5) Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data.

(6) To this end, it is necessary to set up a system known as *Eurodac*, consisting of a Central System, which will operate a computerised central database of fingerprint data, as well as of the electronic means of transmission between the Member States and the Central System.

(7) *With a* view *to* ensuring equal treatment for all applicants *for* and beneficiaries of international protection, as well as in order to ensure consistency with *the* current EU asylum acquis*,* in particular with 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[2] and 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], it is appropriate to *extend* the scope of this Regulation *in* order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

(8) It is also necessary to require the Member States promptly to take and transmit fingerprint data of every applicant for international protection and of every *third-country* national or stateless person who is apprehended in connection with the irregular crossing of an external border of a Member State, if they are at least 14 years of age.

(9) It is necessary to lay down precise rules on the transmission of such fingerprint data to the Central System, the recording of such fingerprint data and other relevant data in the Central System, their storage, their comparison with other fingerprint data, the transmission of the results of such comparison and the ***marking*** and erasure of the recorded data. Such rules may be different for, and should be specifically adapted to, the situation of different categories of ***third-country nationals*** or stateless persons.

(10) *Third-country* nationals or stateless persons who have requested international protection

---

1 *OJ L ...*

2 *OJ L 304, 30.9.2004, p. 12.*

in one Member State may have the option of requesting international protection in another Member State for many years to come. Therefore, the maximum period during which fingerprint data should be kept by the Central System should be of considerable length. Given that most *third-country* nationals or stateless persons who have stayed in the Community for several years will have obtained a settled status or even citizenship of a Member State after that period, a period of ten years should be considered a reasonable period for the *storage* of fingerprint data.

(11) The *storage* period should be shorter in certain special situations where there is no need to keep fingerprint data for that length of time. Fingerprint data should be erased immediately once third-country nationals or stateless persons obtain citizenship of a Member State ***or a long- term residence permit in a Member State in accordance with Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents[1].***

(12) It is appropriate to store data relating to those data subjects whose fingerprints were initially recorded in *Eurodac on* lodging their applications for international protection and who have been granted international protection in a Member State in order to allow data recorded *on* lodging an application for international protection to be *compared with* them.

(13) For a transitional period the Commission should remain responsible for the management of the Central System and for the Communication Infrastructure. In the long term, and following an impact assessment *including* a substantive analysis of alternatives from *a* financial, operational and organisational perspective, a Management Authority with responsibility for these tasks should be established.

(14) It is necessary to lay down clearly the respective responsibilities of the Commission and the Management Authority, in respect of the Central System and the Communication Infrastructure, and of the Member States, as regards data use, data security, access to, and correction of, recorded data.

(15) While the non-contractual liability of the Community in connection with the operation of the *Eurodac* system will be governed by the relevant provisions of the Treaty, it is necessary to lay down specific rules for the non-contractual liability of the Member States in connection with the operation of the system.

(16) *Since* the objective of *this Regulation*, namely the creation of a system for the comparison of fingerprint data to assist the implementation of the Community's asylum policy, cannot ‖ be sufficiently achieved by the Member States and*, given its scale and effects,* can therefore be better achieved *at* Community *level, the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty*. In accordance with the principle of proportionality*,* as set out in *that* Article, this Regulation does not go beyond what is necessary *in order* to achieve that objective.

(17) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2] applies to the processing of personal data by the Member

---

1 ***OJ L 16, 23.1.2004, p. 44.***

2 OJ L 281, 23.11.1995, p. 31.

States carried out in application of this Regulation.

(18) The principles set out in Directive 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data should be supplemented or clarified, in particular as far as certain sectors are concerned.

(19) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[1] ***applies to the processing of personal data by the Community institutions and bodies carried out pursuant to this Regulation***. However, certain ***points*** should be clarified in respect of the responsibility for the processing of data and of ***the*** supervision of data protection.

(20) It is appropriate that national supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, *while* the European Data Protection Supervisor, appointed pursuant to Decision 2004/55/EC of the European Parliament and of the Council ‖ [2], should monitor the activities of the Community institutions and bodies in relation to the processing of personal data in view of the limited tasks of the Community institutions and bodies with regard to the data themselves.

(21) It is appropriate to monitor and evaluate the performance of *Eurodac* at regular intervals.

(22) Member States should provide for a system of ***effective, proportionate and dissuasive*** penalties to sanction the use of data ***entered*** in the Central System contrary to the purpose of *Eurodac*.

(23) It is necessary that Member States *be* informed of the status of particular asylum procedures, with a view to facilitating the adequate 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].

(24) This Regulation respects and *should* be applied in accordance with the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation seeks to ensure full respect for the protection of personal data and the right to asylum and to promote the application of Articles 8 and 18 of the Charter.

(25) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope 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],

---

1 OJ L 8, 12.1.2001, p. 1.

2 OJ L 12, 17.1.2004, p. 47.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose of *Eurodac*

1. A system known as *Eurodac* is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to 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] for examining an application for international protection lodged in a Member State by a *third-country* national or stateless person, and otherwise to facilitate the application of the *above* Regulation under the conditions set out in this Regulation.

2. Without prejudice to the use of data intended for *Eurodac* by the Member State of origin in databases set up under *that Member State*'s national law, fingerprint data and other personal data may be processed in *Eurodac* only for the purposes set out in *Article 33(1)* 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]*.

Article 2

Definitions

1. For the purposes of this Regulation:

   (a) 'the Dublin Regulation' means 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];

   (b) an 'applicant for international protection' means a third-country national or a stateless person who has made an application for international protection in respect of which a final decision has not yet been taken;

   (c) 'Member State of origin' means:

      (i) in relation to a person covered by Article 6, the Member State which transmits the personal data to the Central System and receives the results of the comparison;

      (ii) in relation to a person covered by Article 10, the Member State which transmits the personal data to the Central System ;

(iii) in relation to a person covered by Article 13, the Member State which transmits such data to the Central System and receives the results of the comparison;

(d) 'person granted international protection' means a *third-country* national or a stateless person recognised as in need of international protection as defined in Article 2(a) of ‖ Directive 2004/83/EC;

(e) 'hit' *means* the existence of a match or matches established by the Central System by comparison between fingerprint data recorded in the database and those transmitted by a Member State with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 17(4).

2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation.

3. Unless stated otherwise, the terms defined in Article 2 of the Dublin Regulation shall have the same meaning in this Regulation.

Article 3

System architecture and basic principles

1. *Eurodac* shall consist of:

(a) a computerised central fingerprint database (Central System) composed of

– a Central Unit,

– a Business Continuity System*;*

(b) a communication infrastructure between the *Central System* and Member States that provides an encrypted virtual network dedicated to *Eurodac* data (Communication Infrastructure).

2. Each Member State shall have a single designated national data system (National Access Point) which communicates with the Central System.

3. Data on persons covered by *Articles* 6, 10 and 13 which are processed in the Central System shall be processed on behalf of the Member State of origin under the conditions set out in this Regulation and separated by appropriate technical means.

4. The rules governing *Eurodac* shall also apply to operations effected by the Member States as from the transmission of data to the Central System until use is made of the results of the comparison.

5. The procedure for taking fingerprints shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child.

Article 4

Operational management by the Management Authority

1. After a transitional period, a Management Authority, funded from the general budget of the European Union, shall be responsible for the operational management of *Eurodac*. The Management Authority shall ensure, in cooperation with the Member States, that at all times the best available ***techniques***, subject to a cost-benefit analysis, ***are*** used for the Central System.

2. The Management Authority shall also be responsible for the following tasks relating to the Communication Infrastructure:

   (a) supervision;

   (b) security;

   (c) the coordination of relations between the Member States and the provider.

3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:

   (a) tasks relating to implementation of the budget;

   (b) acquisition and renewal;

   (c) contractual matters.

4. During a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for the operational management of *Eurodac*.

5. Operational management of *Eurodac* shall consist of all the tasks necessary to keep *Eurodac* functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for *interrogating* the Central System.

6. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Communities, the Management Authority shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with *Eurodac* data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

7. The Management Authority referred to in this Regulation shall be the Management Authority competent for ***Eurodac,*** SIS II and VIS.

8. The setting-up of the Management Authority and the interoperability of the several databases for which it has competence shall be without prejudice to the separate and discrete operation of those databases.

Article 5

Statistics

The Management Authority shall draw up statistics on the work of the Central System every month, indicating in particular:

(a) the number of data sets transmitted on applicants for international protection and the persons referred to in Articles 10 and 13 ;

(b) the number of hits for applicants for international protection who have lodged an application for international protection in another Member State;

(c) the number of hits for persons referred to in Article 10 who have subsequently lodged an application for international protection;

(d) the number of hits for persons referred to in Article 13 who had previously lodged an application for international protection in another Member State;

(e) the number of fingerprint data which the Central System had to repeatedly request from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;

(f) the number of data sets marked in accordance with Article 14(1);

(g) the number of hits for persons referred to in Article 14(1).

At the end of each year, statistical data shall be established in the form of a compilation of the monthly statistics for that year, including an indication of the number of persons for whom hits have been recorded under (b), (c)***,*** (d) ***and (g)***.

The statistics shall contain a breakdown of data for each Member State.

CHAPTER II

APPLICANTS FOR INTERNATIONAL PROTECTION

Article 6

Collection, transmission and comparison of ***fingerprint data***

1. Each Member State shall***, no later than 48 hours*** after the lodging of an application as defined by Article 20(2) of the Dublin Regulation***,*** take the fingerprints of all fingers of every applicant for international protection of at least 14 years of age and shall, no later than ***24 hours*** after the ***taking of the fingerprints,*** transmit ***the fingerprint data*** together with the data referred to in points (b) to (g) of Article 7 ***of this Regulation*** to the Central System.

By way of exception, in cases where the fingerprints are seriously, but only temporarily, damaged and cannot provide suitable fingerprint data or in cases where there is a need to enforce a quarantine period because of severe contagious disease, the period of 48 hours for taking the fingerprints of applicants for international protection, as referred to in this paragraph, may be extended up to a maximum of three weeks. Member States may also extend the period of 48 hours in well-founded and proven cases of force majeure for as long as those circumstances persist. The period of 24 hours for transmitting the required data shall apply accordingly.

2. By way of derogation from paragraph 1, when an applicant for international protection arrives in the ▌Member State ***responsible for examining an application for international protection*** following a transfer pursuant to ***Article 23 of*** the Dublin Regulation, the responsible Member State shall ***indicate*** only ‖ the fact of the successful transfer ***with regard to*** the relevant data recorded in the Central System pursuant to ***Article 7 of this Regulation***, in conformity with the requirements for electronic communication with the Central System established by the Management Authority. This information shall be stored in accordance with Article 8 for the purpose of transmission under ***paragraph 6 of this Article***.

3. The Member State which assumes responsibility in accordance with Article 17 of the Dublin Regulation shall indicate that fact with regard to the relevant data recorded in the Central System pursuant to Article 7 of this Regulation, in conformity with the requirements for electronic communication with the Central System established by the Management Authority. This information shall be stored in accordance with Article 8 for the purpose of transmission under paragraph 6 of this Article.

4. Fingerprint data within the meaning of point (a) of Article 7, transmitted by any Member State, shall be compared automatically with the fingerprint data transmitted by other Member States and already stored in the Central System.

5. The Central System shall ensure, on the request of a Member State, that the comparison referred to in *paragraph 4* covers the fingerprint data previously transmitted by that Member State, in addition to the data from other Member States.

6. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin. Where there is a hit, it shall transmit for all data sets corresponding to the hit, the data referred to in *points (a) to* ***(g)*** *of* Article 7 ‖ along with, where appropriate, the mark referred to in Article 14(1).

Article 7

Recording of data

Only the following data shall be recorded in the Central System:

(a) fingerprint data;

(b) Member State of origin, place and date of the application for international protection;

(c) sex;

(d) reference number used by the Member State of origin;

(e) date on which the fingerprints were taken;

(f) date on which the data were transmitted to the Central System;

(g) operator user ID.

Article 8

Data storage

Each set of data as referred to in Article 7 shall be stored in the *Central* System for ten years from the date on which the fingerprints were taken.

On expiry of *that* period, the Central System shall automatically erase the data from the *Central* System.

Article 9

Advance data erasure

1. Data relating to a person who has acquired citizenship of any Member State ***or has been issued a long-term residence permit by a Member State in accordance with Directive 2003/109/EC*** before *the* expiry of the period referred to in Article 8 *of this Regulation* shall be erased from the Central System in accordance with Article 20(3) as soon as the Member State of origin becomes aware that the person has acquired such citizenship ***or has been issued such a permit***.

2. The Central System shall inform all Member States of origin about the ***erasure*** of data ***for the reason specified in paragraph 1*** by another Member State of origin having produced a hit with data ***which they*** transmitted relating to persons referred to in Article 6 or ‖ 10.

CHAPTER III

THIRD-COUNTRY NATIONALS OR STATELESS PERSONS APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER

Article 10

Collection and transmission of fingerprint data

1. Each Member State shall, in accordance with the safeguards laid down in the European Convention *for the Protection of* Human Rights *and Fundamental Freedoms* and in the United Nations Convention on the Rights of the Child, ▌take the fingerprints of all fingers of every third-country national or stateless person of at least 14 years of age who

is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back***, no later than 48 hours from the date of apprehension.***

2. The Member State concerned shall no later than ***24 hours after the taking of the fingerprints of the third-country national or stateless person, as referred to in paragraph 1,*** transmit ‖ the following data in relation to ***that person*** *to the Central System:*

(a) fingerprint data;

(b) Member State of origin, place and date of apprehension;

(c) sex;

(d) reference number used by the Member State of origin;

(e) date on which the fingerprints were taken;

(f) date on which the data were transmitted to the Central System;

(g) operator user ID.

By way of exception, in cases where the fingerprints are seriously, but only temporarily, damaged and cannot provide suitable fingerprint data or in cases where there is a need to enforce a quarantine period because of severe contagious disease, the period of 48 hours for taking the fingerprints of the third-country national or stateless person, as referred to in paragraph 1, may be extended up to a maximum of three weeks. Member States may also extend the period of 48 hours in well-founded and proven cases of force majeure for as long as those circumstances persist. The period of 24 hours for transmitting the required data shall apply accordingly.

Article 11

Recording of data

1. The data referred to in Article 10(2) shall be recorded in the Central System.

Without prejudice to Article 5, data transmitted to the Central System pursuant to Article 10(2) shall be recorded for the sole purpose of comparison with data on applicants for international protection transmitted subsequently to the Central System.

The Central System shall not compare data transmitted to it pursuant to Article 10(2) with any data previously recorded in the Central System, *or* with data subsequently transmitted to the Central System pursuant to Article 10(2).

2. As regards the comparison of data on applicants for international protection subsequently transmitted to the Central System with the data referred to in paragraph 1, the procedures provided for in *Article 6(4)* and *(6)* shall apply.

Article 12

Storage of data

1. Each set of data relating to a *third-country* national or stateless person as referred to in Article 10(1) shall be stored in the Central System for one year from the date on which the fingerprints of the *third-country* national or stateless person were taken. *On* expiry of *that* period, the Central System shall automatically erase the data from the Central System.

2. The data relating to a *third-country* national or stateless person as referred to in Article 10(1) shall be erased from the Central System in accordance with ***Article 20(3) as soon as*** the Member State of origin becomes aware of one of the following circumstances before the ▌ period mentioned in paragraph 1 *of this Article* has expired:

   (a) the *third-country* national or stateless person has been issued with a residence permit;

   (b) the *third-country* national or stateless person has left the territory of the Member States;

   (c) the *third-country* national or stateless person has acquired the citizenship of any Member State.

3. The Central System shall inform all Member States of origin about the ***erasure*** of data for the reason specified in paragraph 2(a) ***or*** (b) by another Member State of origin having produced a hit with data ***which they*** transmitted relating to persons referred to in Article 10.

4. The Central System shall inform all Member States of origin about the ***erasure*** of data for the reason specified in paragraph 2(c) by another Member State of origin having produced a hit with data ***which they*** transmitted relating to persons referred to in Article 6 or ‖ 10.

CHAPTER IV

THIRD-COUNTRY NATIONALS OR STATELESS PERSONS FOUND ILLEGALLY PRESENT IN A MEMBER STATE

Article 13

Comparison of fingerprint data

1. With a view to checking whether a *third-country* national or a stateless person found illegally present within its territory has previously lodged an application for international protection in another Member State, each Member State may transmit to the Central System any fingerprint data relating to fingerprints which it may have taken of any such *third-country* national or stateless person of at least 14 years of age together with the reference number used by that Member State.

   As a general rule there are grounds for checking whether the *third-country* national or stateless person has previously lodged an application for asylum international protection in another Member State where:

(a) the *third-country* national or stateless person declares that he/she has lodged an application for international protection but without indicating the Member State in which he/she *lodged* the application;

(b) the *third-country* national or stateless person does not request international protection but objects to being returned to his/her country of origin by claiming that he/she would be in danger; or

(c) the *third-country* national or stateless person otherwise seeks to prevent his/her removal by refusing to cooperate in establishing his/her identity, in particular by showing no, or false, identity papers.

2. Where Member States take part in the procedure referred to in paragraph 1, they shall transmit to the Central System the fingerprint data relating to all or at least the index fingers and, if those are missing, the prints of all other fingers, of *third-country* nationals or stateless persons *as* referred to in paragraph 1.

3. The fingerprint data of a *third-country* national or a stateless person as referred to in paragraph 1 shall be transmitted to the Central System solely for the purpose of comparison with the fingerprint data of applicants for international protection transmitted by other Member States and already recorded in the Central System.

The fingerprint data of such a *third-country* national or a stateless person shall not be recorded in the Central System, nor shall they be compared with the data transmitted to the Central System pursuant to Article 10(2).

4. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for international protection transmitted by other Member States which have already been stored in the Central System, the procedures provided for in *Article 6(4)* and *(6)* shall apply.

CHAPTER V

PERSONS GRANTED INTERNATIONAL PROTECTION

Article 14

Marking of data

1. The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to ***Article 7*** in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Management Authority. *That* mark shall be stored in the Central System in accordance with Article 8 for the purpose of transmission under *Article 6(6)*.

2. The Member State of origin shall unmark data concerning a third-country national or stateless person whose data were previously marked in accordance with paragraph 1 if *his/her* status is revoked or ended or renewal of *his/her* status is refused under Article 14 or 19 of ‖ Directive 2004/83/EC***, or if he/she ceases to be a refugee or to be eligible for subsidiary protection under Articles 11 and 16 respectively of that Directive***.

CHAPTER VI

DATA USE, DATA PROTECTION AND LIABILITY

Article 15

Responsibility for data use

1. The Member State of origin shall be responsible for ensuring that:

   (a) fingerprints are taken lawfully;

   (b) fingerprint data and the other data referred to in Article 7, Article 10(2) and Article 13(2) are lawfully transmitted to the Central System;

   (c) data are accurate and up-to-date when they are transmitted to the Central System;

   (d) without prejudice to the responsibilities of the Commission, data in the Central System are lawfully recorded, stored, corrected and erased;

   (e) the results of fingerprint data comparisons transmitted by the Central System are lawfully used.

2. In accordance with Article 19, the Member State of origin shall ensure the security of the data referred to in paragraph 1 before and during *their* transmission to the Central System, as well as the security of the data *which* it receives from the Central System.

3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article 17(4).

4. The Commission shall ensure that the Central System is operated in accordance with the provisions of this Regulation. In particular, the Commission shall:

   (a) adopt measures ensuring that persons working with the Central System use the data recorded therein only in accordance with the purpose of *Eurodac* as laid down in Article 1(1);

   (b) take the necessary measures to ensure the security of the Central System in accordance with Article 19;

   (c) ensure that only persons authorised to work with the Central System have access thereto, without prejudice to the competences of the European Data Protection Supervisor.

   The Commission shall inform the European Parliament and the Council of the measures *which* it takes pursuant to the first subparagraph.

Article 16

Transmission

1. Fingerprints shall be digitally processed and transmitted in the data format referred to in Annex I. As far as is necessary for the efficient operation of the Central System, the Management Authority shall establish the technical requirements for *the* transmission of the data format by Member States to the Central System and vice versa. The Management Authority shall ensure that the fingerprint data transmitted by the Member States can be compared by the computerised fingerprint recognition system.

2. Member States ***shall*** transmit the data referred to in Article 7, Article 10(2) and Article 13(2) electronically. The data referred to in Article 7 and Article 10(2) shall be automatically recorded in the Central System. As far as is necessary for the efficient operation of the Central System, the Management Authority shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central System and vice versa.

3. The reference number referred to in Article 7(d)***,*** Article 10(2)(d) ***and Article 13(1)*** shall make it possible to relate data unambiguously to one particular person and to the Member State which ***transmitted*** the data. In addition, it shall make it possible to *determine* whether such data relate to a person referred to in Article 6, ‖ 10 or ‖ 13.

4. The reference number shall begin with the identification letter or letters by which, in accordance with the norm referred to in Annex I, the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person. '1' refers to data relating to persons referred to in Article 6, '2' to persons referred to in Article 10 and '3' to persons referred to in Article 13.

5. The Management Authority shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central System.

6. The Central System shall confirm receipt of the transmitted data as soon as possible. To this end the Management Authority shall establish the necessary technical requirements to ensure that Member States receive the receipt *confirmation* if requested.

Article 17

Carrying out comparisons and transmitting results

1. Member States shall ensure the transmission of fingerprint data in an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. As far as is necessary to ensure that the results of the comparison by the Central System reach a very high level of accuracy, the Management Authority shall define the appropriate quality of transmitted fingerprint data. The Central System shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data do not lend themselves to comparison using the computerised fingerprint recognition system, the Central System shall request the Member State to transmit fingerprint data of the appropriate quality.

2. The Central System shall carry out comparisons in the order of arrival of requests. Each request *shall* be dealt with within 24 hours. ▌A Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where *such* time *limits* cannot be respected owing to circumstances which are outside the Management Authority's responsibility*,* the Central System shall

process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as is necessary for the efficient operation of the Central System, the Management Authority shall establish criteria to ensure the priority handling of requests.

3. As far as is necessary for the efficient operation of the Central System, the Management Authority shall establish the operational procedures for the processing of the data received and for transmitting the *results* of the comparison.

4. The results of the comparison shall immediately *be* checked in the Member State of origin. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to *Article 33* of the Dublin Regulation.

   Information received from the Central System relating to other data found to be unreliable shall be erased ▌ as soon as the unreliability of the data is established.

5. Where final identification in accordance with paragraph 4 *reveals* that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the Commission***,*** to the Management Authority ***and to the European Data Protection Supervisor***.

▌

Article 18

Communication between Member States and the Central System

Data transmitted from the Member States to the Central System and vice versa shall use the Communication Infrastructure to be provided by the Management Authority. As far as is necessary for the efficient operation of the Central System, the Management Authority shall establish the technical procedures necessary for the use of the Communication Infrastructure.

Article 19

Data security

1. The Member State ***of origin*** shall ensure the security of the data before and during transmission to the Central System. Each Member State shall ensure the security of the data which it receives from the Central System.

2. Each Member State shall, in relation to its national system, adopt the necessary measures, including a security plan, in order to:

   (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

   (b) deny unauthorised persons access to national installations in which the Member State carries out operations in accordance with the purpose of *Eurodac* (checks at entrance to the installation);

(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(e) prevent the unauthorised processing of data in *Eurodac* and any unauthorised modification or deletion of data processed in *Eurodac* (control of data entry);

(f) ensure that persons authorised to access *Eurodac* have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);

(g) ensure that all authorities with a right of access to *Eurodac* create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make *those* profiles available to the *national supervisory authorities* referred to in Article 24 without delay at their request (personnel profiles);

(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

(i) ensure that it is possible to verify and establish what data have been processed in *Eurodac*, when, by whom and for what purpose (control of data recording);

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from *Eurodac* or during the transport of data media, in particular by means of appropriate encryption techniques (transport control);

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).

3. ***All the authorities that participate in the Eurodac system shall prevent access to or the transfer of data recorded in Eurodac to the authorities of any unauthorised third country, especially to the State of origin of the persons covered by this Regulation.***

4. The Management Authority shall take the necessary measures in order to achieve the objectives set out in paragraph 2 as regards the operation of *Eurodac*, including the adoption of a security plan.

5. ***The Management Authority shall lay down a common set of requirements to be fulfilled by persons in order to be granted authorisation to access Eurodac.***

Article 20

Access to, and correction or erasure of, data recorded in *Eurodac*

1. The Member State of origin shall have access to *the* data which it has transmitted and which are recorded in the Central System in accordance with the provisions of this

Regulation.

No Member State may conduct searches in the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in *Article 6(6)*.

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the Central System shall be those designated by each Member State for the purpose of Article 1(1). *That* designation shall specify the *precise* unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and the Management Authority a list of those authorities and any amendments thereto***, in the case of amendments at the latest 30 days after the list was amended***. The Management Authority shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Management Authority shall publish once a year an updated consolidated list.

3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central System by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out *pursuant to* Article 8 or Article 12(1).

4. If a Member State or the Management Authority has evidence to suggest that data recorded in the Central System are factually inaccurate, it shall advise the Member State of origin as soon as possible.

   If a Member State has evidence to suggest that data were recorded in the Central System *in breach of* this Regulation, it shall advise the Commission and the Member State of origin as soon as possible. The *Member State of origin* shall check the data concerned and, if necessary, *correct* or erase them without delay.

5. The Management Authority shall not transfer or make available to the authorities of any third country data recorded in the Central System, unless it is specifically authorised to do so within the framework of a Community agreement on the criteria and mechanisms for determining the State responsible for examining an application for international protection.

Article 21

Keeping of records

1. The Management Authority shall keep records of all data processing operations within the Central System. These records shall show the purpose of access, the date and time, the data transmitted, the data used for interrogation and the name of both the unit entering or retrieving the data and the persons responsible.

2. Such records may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security pursuant to Article 19. The records ***shall*** be protected by appropriate measures against unauthorised access and erased after a period of one year after the ***storage*** period referred to in Article 8 and in Article 12(1) has expired, if they are not required for monitoring procedures which have already begun.

3. Each Member State shall take the necessary measures in order to achieve the objectives set out in *paragraphs* 1 and 2 in relation to its national system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.

Article 22

Liability

1. Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with the provisions *of* this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That *Member* State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event giving rise to the damage.

2. If *the* failure of a Member State to comply with its obligations under this Regulation causes damage to the Central System, that Member State shall be liable for such damage, unless and insofar as the Management Authority or another Member State failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State.

Article 23

Rights of the data subject

1. A person covered by this Regulation shall be informed by the Member State of origin in writing, and where appropriate, orally, in a language which *he/she* ***understands or may*** reasonably ***be presumed*** to understand, of the following:

   (a) the identity of the controller and of his representative, if any;

   (b) ▌the purpose for which ▌data ***relating to him/her*** will be processed within *Eurodac,* including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation;

   (c) the recipients of the data;

   (d) in relation to a person covered by Article 6 or ‖ 10, the obligation to have his/her fingerprints taken;

   (e) ▌the right of access to data relating to ***him/her***, and the right to request that inaccurate data relating to ***him/her*** be corrected or that unlawfully processed data relating to ***him/her*** be ***erased***, ***as well as*** the procedures for exercising those rights***, including*** the contact details ***of the controller and*** of the *national supervisory authorities* referred to in ***Article 24***, which shall hear claims concerning the protection of personal data.

   In relation to a person covered by Article 6 or ‖ 10, the information referred to in the

first subparagraph shall be provided when his/her fingerprints are taken.

In relation to a person covered by Article 13, the information referred to in the first subparagraph shall be provided no later than the time when the data relating to *that* person are transmitted to the Central System. This obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.

Where the ***person covered by this Regulation*** is a minor, Member States shall provide the information in an age-appropriate manner.

2. In each Member State, any data subject may, in accordance with the laws, regulations and procedures of that *Member* State, exercise the rights provided for in Article 12 of Directive 95/46/EC.

   Without prejudice to the obligation to provide other information in accordance with point (a) of Article 12 of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him/her recorded in the Central System and of the Member State which transmitted them to the Central System. Such access to data may be granted only by a Member State.

3. In each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be carried out without excessive delay by the Member State which transmitted the data, in accordance with its laws, regulations and procedures.

4. If the rights of correction and erasure are exercised in a Member State other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of *the transmitting* Member State or States, so that the *transmitting Member State or States* may check the accuracy of the data and the lawfulness of their transmission and recording in the Central System.

5. If it emerges that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall correct or erase the data in accordance with Article 20(3). That Member State shall confirm in writing to the data subject without excessive delay that it has taken action to correct or erase data relating to him/her.

6. If the Member State which transmitted the data does not agree that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject without excessive delay why it is not prepared to correct or erase the data.

   That Member State shall also provide the data subject with information explaining the steps which he/she can take if he/she does not accept the explanation provided. This shall include information on how to bring an action or, if appropriate, a complaint before the competent authorities or courts of that Member State and any financial or other assistance that is available in accordance with the laws, regulations and procedures of that Member State.

7. Any request under paragraphs 2 and 3 shall contain all the necessary particulars to

identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the rights referred to in paragraphs 2 and 3 and shall be destroyed immediately afterwards.

8. The competent authorities of the Member States shall cooperate actively to enforce promptly the rights laid down in paragraphs 3, 4 and 5.

9. Whenever a person requests data relating to *him/her* in accordance with ***paragraph 2***, the competent authority shall keep a record in the form ***of*** a written document that such a request was made, and shall make *that* document available to the *national supervisory authorities* referred to in ***Article 24*** without delay, *at* their request.

10. In each Member State, the national supervisory authority shall assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his/her rights.

11. The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall assist and, where requested, advise him/her in exercising his/her right to correct or erase data. Both national supervisory authorities shall cooperate to this end. Requests for such assistance may be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data.

12. In each Member State, any person may, in accordance with the laws, regulations and procedures of that *Member* State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the *Member* State if he/she is refused the right of access provided for in paragraph 2.

13. Any person may, in accordance with the laws, regulations and procedures of the Member State which transmitted the data, bring an action or, if appropriate, a complaint before the competent authorities or courts of that *Member* State concerning the data relating to him/her recorded in the Central System, in order to exercise his/her rights under paragraph 3. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject in accordance with paragraph 11 shall subsist throughout the proceedings.

Article 24

Supervision by the National Supervisory Authority

1. Each Member State shall provide that the national supervisory authority or authorities designated pursuant to Article 28(1) of Directive 95/46/EC shall monitor independently, in accordance with its national law, the lawfulness of the processing, in accordance with this Regulation, of personal data by the Member State in question, including their transmission to the Central System.

2. Each Member State shall ensure that its national supervisory authority *or authorities* has access to advice from persons with sufficient knowledge of fingerprint data.

Article 25

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall check that the personal data processing activities of the Management Authority are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly. ***The European Data Protection Supervisor may request any information from the Management Authority considered necessary to carry out the functions entrusted to it under that Regulation.***

2. The European Data Protection Supervisor shall ensure that an audit of the Management Authority's personal data processing activities is carried out in accordance with international auditing standards at least every four years. A report of such audit shall be sent to the European Parliament, the Council, *the Commission,* the Management Authority ‖ and the *national supervisory authorities*. The Management Authority shall be given an opportunity to make comments before the report is adopted.

Article 26

Cooperation between National Supervisory Authorities and the European Data Protection Supervisor

1. The *national supervisory authorities* and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of *Eurodac*.

2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

3. The *national supervisory authorities* and the European Data Protection Supervisor shall meet for that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Management Authority every two years.

CHAPTER VII

FINAL PROVISIONS

Article 27

Costs

1. The costs incurred in connection with the establishment and operation of the Central System and the Communication Infrastructure shall be borne by the general budget of the European Union.

2. The costs incurred by national units and the costs for their connection to the Central System shall be borne by each Member State.

Article 28

Annual report: monitoring and evaluation

1. The Management Authority shall submit to the European Parliament and the Council an annual report on the activities of the Central System. The annual report shall include information on the management and performance of *Eurodac in relation to* pre-defined quantitative indicators for the objectives referred to in paragraph 2.

2. The Management Authority shall ensure that procedures are in place to monitor the functioning of the Central System *in relation to* objectives relating to output, cost-effectiveness and quality of service.

3. For the purposes of technical maintenance, reporting and statistics, the Management Authority shall have access to the necessary information relating to the processing operations performed in the Central System.

4. Every two years, the Management Authority shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the Central System, including *its* security.

5. Three years after the start of application of this Regulation as provided for in Article 33(2) and every four years thereafter, the Commission shall produce an overall evaluation of *Eurodac*, examining *the* results achieved *in relation to* objectives and assessing the continuing validity of the underlying rationale, the application of this Regulation in respect of the Central System, the security of the Central System, and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council.

6. Member States shall provide the Management Authority and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5.

7. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.

Article 29

Penalties

Member States shall take the necessary measures to ensure that any use of data entered in the Central System contrary to the purpose of *Eurodac* as laid down in Article 1(1) is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive.

Article 30

Territorial scope

The provisions of this Regulation shall not be applicable to any territory to which the Dublin Regulation does not apply.

Article 31

Transitional provision

Data blocked in the Central System in accordance with Article 12 of ‖ Regulation (EC) No *2725/2000* shall be unblocked and marked in accordance with Article 14(1) of this Regulation on the date provided for in Article 33(2).

Article 32

Repeal

Regulations (EC) No 2725/2000 ‖ and ‖ (EC) No 407/2002 ‖ are *hereby* repealed with effect from the date provided for in Article 33(2) *of this Regulation*.

References to the repealed Regulations shall be *construed as references to this Regulation and be* read in accordance with the correlation table in *Annex III*.

Article 33

Entry into force and applicability

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. This Regulation shall apply from the date which the Commission shall publish in the Official Journal of the European Union, when the following conditions are met:

   (a) each Member State has notified the Commission that it has made the necessary technical arrangements to transmit data to the Central System in accordance with this Regulation*;* and

   (b) the Commission has made the necessary technical arrangements for the Central System to begin operations in accordance with this Regulation.

3. Member States shall notify the Commission as soon as the arrangements referred to in paragraph 2(a) have been made, ***which shall*** in any event ***be*** no later than 12 months from the date of the entry into force of this Regulation.

4. During the transitional period referred to in Article 4(4), references in this Regulation to the Management Authority shall be construed as references to the Commission.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaty establishing the European Community.

Done at ‖

For the European Parliament	For the Council
The President	The President

ANNEX I

Data format for the exchange of fingerprint data

The following format is prescribed for the exchange of fingerprint data:

ANSI/NIST-ITL 1a-1997, Ver.3, June 2001 (INT-1) and any future further developments of this standard.

Norm for Member State identification letters

The following ISO norm will apply: ISO 3166 - 2 letters code.

ANNEX II

Repealed Regulations
(referred to in Article 32)

Council Regulation (EC) No *2725/2000*	(OJ L 316, 15.12.2000, p. 1.)
Council Regulation (EC) No *407/2002*	(OJ L *62*, *5.3*.2002*,* p. 1.)

ANNEX III

Correlation table

Regulation *(EC) No 2725/2000*	This Regulation
Article 1(1)	Article 1(1)
Article 1(2), first subparagraph	Article 3(1)
Article 1(2), second subparagraph	Article 3(4)
Article 1(3)	Article 1(2)
Article 2	*Article 2*

Article 3(1)	*Article 3(1)*
‖	‖
Article 3(2)	Article 3(3)
Article 3(3)	Article 5
Article 3(4)	-
Article 4(1)	Article 6(1)
Article 4(2)	-
Article 4(3)	*Article 6(4)*
Article 4(4)	*Article 6(5)*
Article 4(5)	*Article 6(6)*
Article 4(6)	Article 17(4)
Article 4(7)	-
Article 5	Article 7
Article 6	Article 8
Article 7	Article 9
Article 8	Article 10
Article 9	Article 11
Article 10	Article 12
Article 11(1)-(4)	Article 13(1)-(4)
Article 11(5)	-
Article 12	Article 14
Article 13	Article 15
Article 14	Article 19
Article 15	Article 20
Article 16	Article 21

Article 17	Article 22
Article 18	Article 23
Article 19	Article 24
Article 20	Article 25
Article 21	Article 27
Article 22	-
‖	‖
Article 23	-
Article 24	Article 28
Article 25	Article 29
Article 26	Article 30
Article 27	Article 33
-	Annex II
Regulation *(EC) No 407/2002*	This Regulation
Article 1	-
Article 2	Article 16
Article 3	Article 17
Article 4	Article 18
Article 5(1)	*Article 3(3)*
Annex I	Annex I
Annex II	-