COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 10.9.2009
COM(2009) 344 final

2009/0130 (CNS)

Proposal for a

COUNCIL DECISION

on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes

{COM(2009) 342 final}
{SEC(2009) 936}
{SEC(2009) 937}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

- **Grounds for and objectives of the proposal**

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

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

Fingerprint data of asylum seekers are collected and stored in the Member State in which the asylum application was filed, as well as in EURODAC. In all Member States that replied to the questionnaire of the Commission services, the law enforcement authorities had direct or indirect access to their national databases that contain the fingerprints of asylum seekers for the purpose of fighting crime. During the consultation of experts it became clear that those national law enforcement authorities that consult national databases containing fingerprints of asylum seekers for criminal investigations consider the hit rate significant.

However, while Member States successfully access asylum seekers fingerprints on a national level, it seems that access to asylum seekers fingerprint databases of other Member States is more problematic. The reason is that there is a structural information and verification gap since there is currently no single system that is accessible to law enforcement authorities which enables to determine the Member State that has information on an asylum seeker. If a query of a national Automated Fingerprint Identification Systems (AFIS) using the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision) which will be implemented by Member States by June 2011 does not result in a "hit", it is not certain that no information is available in a Member State. Therefore, law enforcement authorities will not only remain ignorant about whether or not information is available at all and in which Member State, but often also whether this information relates to the same person. Law enforcement officials will only know whether information is available in a database of another Member State if their judicial authorities issue a request for mutual legal assistance requesting the other Member State to query their databases and send the relevant information.

- **General context**

The Hague Programme stated that the exchange of information to strengthen security should be improved. One of the ideas contained in the Programme is to make full use of new technology, inter alia - where appropriate - by direct (on-line) access for law

enforcement authorities, including for Europol, to existing central EU databases.

The conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 considered that, in order to fully achieve the aim of improving security and to enhance the fight against terrorism, access under certain conditions to EURODAC should be granted to Member States' police and law enforcement authorities, as well as Europol, in the course of their duties in relation to the prevention, detection and investigation of terrorist offences and other serious criminal offences. It therefore invited the Commission to present as soon as possible the necessary proposals to achieve this aim.

The absence of the possibility for law enforcement authorities to access EURODAC to combat terrorism and other serious crime was also reported as a shortcoming in the Commission Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 24 November 2005.

The existing instruments on exchange of law enforcement information do not allow to timely determine with sufficient certainty whether a Member State actually holds fingerprint data of an asylum seeker. This means that without any action at EU level, law enforcement authorities will continue to remain ignorant about whether or not information on a fingerprint is available at all, in which Member State information is available, and whether information relates to the same person. Without efficient and reliable means to determine whether or not information is available in another Member State the action of public authorities either becomes prohibitively expensive or seriously jeopardises the application of the law because no further efficient and reasonable action to determine a person's identity can be taken.

- **Existing provisions in the area of the proposal**

Council Regulation (EC) No 2725/2000 of 11 December 2000 established 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (the 'Eurodac' Regulation). On 3 December 2008 the Commission adopted a proposal to amend the EURODAC regulation aimed at making the EURODAC system more efficient.

There are currently some EU instruments that permit consultation of fingerprints and other law enforcement data held by one Member State by another Member State.

The first instrument that is likely to be used for consultations regarding fingerprints is the Prüm Decision.. On the basis of this Council Decision the Member States' grant each other automated access inter alia to national AFISon the basis of a hit/no hit request. If a query on the basis of the Prüm Decision produces a hit, supplementary information, including personal data, can be obtained in the Member State that recorded the fingerprint in its national AFIS using national law , including mutual legal assistance.

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

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

The last instrument that Member States could use is mutual legal assistance under which the judicial authorities of the Member States can seek access to criminal and non-criminal fingerprint collections, including on asylum seekers on the basis of the Convention on Mutual Assistance in Criminal Matters.

The last two instruments cannot be used when the Member State that holds data on a fingerprint is not known. Currently no system exists which could be used to identify such Member State.

- **Consistency with the other policies and objectives of the Union**

The proposal is fully in line with the overall objective of creating a European area of freedom, security and justice. In particular, this proposal was subject to in-depth scrutiny to ensure that its provisions are fully compatible with fundamental rights and notably the right to asylum and the protection of personal data as enshrined respectively in Article 8 (protection of personal data) and 18 (right to asylum) of the Charter of Fundamental Rights of the EU as reflected in the Impact Assessment accompanying this proposal.

With regard to the special situation of persons seeking international protection, the concern was raised that data extracted from EURODAC for law enforcement purposes could end up in the hands of the countries from which the applicants fled and fear persecution. This could have adverse effects on the applicant, his relatives and friends, thus potentially discouraging refugees from formally applying for international protection in the first place. As a result of this scrutiny, the proposal contains a specific prohibition of sharing personal data obtained pursuant to this proposal with third countries, organisations or entities. In addition, an extensive monitoring and evaluation mechanism of the proposal is foreseen. This evaluation will include whether the operation of the Decision will have led to the stigmatisation of persons seeking international protection. Furthermore, to keep the interference with the right to protection of personal data legitimate and proportional, strict access conditions are provided which also exclude that EURODAC fingerprint are searched on a routine basis. The proposal is also fully compatible with data protection principles since the Council Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Co-operation in Criminal Matters 2008/977/JHA applies to it. This Framework Decision lays down the principles that Member States must abide by when processing data retrieved from an EU database, such as EURODAC, while at the same time requires Member States to impose effective sanctions for violations of the data protection principles.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

Consultation methods, main sectors targeted and general profile of respondents

The Commission consulted the States applying the Dublin acquis, i.e. the Member States, Iceland, Norway and Switzerland, as well as to Europol by way of two questionnaires and an expert meeting which took place in Brussels on 25-26 September 2007, during which the experts had the opportunity to clarify the replies to the questionnaire and express further views.

Secondly, the Commission consulted the following intergovernmental organisations, non-governmental organisations and other scientific experts working in the area of asylum law/policy, fundamental rights and protection of personal data during a meeting in Brussels on 8 October 2007. MEPs Cavada, Klamt and Ludford also participated at the same meeting.

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

Summary of responses and how they have been taken into account

The consultation process had a major impact on shaping the legislative proposal. More specifically, such impact affected the choice of the legislative option and the various parameters of the option. The consultations showed that the Member States were very favourable to having the possibility to compare fingerprints with EURODAC for law enforcement purposes, while civil liberties and asylum NGOs were not very favourable. The proposal presents a balance on the positions of the various interested groups, by containing several guarantees and limits.

- **Collection and use of expertise**

There was no need for external expertise.

- **Impact assessment**

The Impact Assessment considered three options, and a number of sub-options. The options was a no action option, a legislative option for making it possible to request the comparison with EURODAC data for law enforcement purposes and a legislative option for making it possible to request the comparison with EURODAC data for law enforcement purposes while at the same time regulating the exchange of supplementary information following a successful 'hit' from EURODAC. A fourth option was originally considered but rejected as it would entail disproportionate costs.

Between the "no action" option and the legislative proposal options, the legislative proposal options present clear advantages. Access of law enforcement authorities to EURODAC is the only timely, accurate, secure and cost-efficient way to identify

whether and if so where data about asylum seekers are available in the Member States. No reasonable efficient alternative exists to EURODAC to establish or verify the exact identity of an asylum seeker that allows law enforcement authorities to obtain the same result. This unique identification is essential for law enforcement authorities in order to prevent and combat terrorism and serious crime involving third country nationals, as well as to protect victims of terrorism or serious crime. Access to 'Eurodac' cannot be considered disproportionate to the aims to be achieved.

Between the two options involving legislative measures, both options present the same impacts on fundamental rights. The third option would make supplementary information on the asylum seeker available between Member States through a special procedure where such is requested, while the second option would use the existing instruments to facilitate access to such supplementary information. Even though the achievement of the objectives would be more effective under the third option, it is considered that the costs of implementing the third option would be higher compared to the second option.

In addition, currently there are no indications that current instruments on exchange of law enforcement information would not be a sufficient instrument for the exchange of supplementary information.

The Commission carried out an impact assessment listed in the Work Programme SEC(2009) 936.

3. LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The proposed action establishes the basis for the right of Member States as well as Europol to request a comparison of fingerprint data or a latent with EURODAC data. A successful comparison with result in a 'hit' reply from EURODAC, which will be acompanied by all data that is held in EURODAC regarding the fingerprint. Requests for supplementary information following a hit would not be regulated in the proposed Council Decision but rather be covered by existing instruments on the exchange of law enforcement information.

The scope of the proposal will be the fight against terrorist offences and serious criminal offences, such as trafficking in human beings and drugs.

Even though currently EURODAC does not provide the possibility to search the database on the basis of a latent, this search facility can be added to the EURODAC system under the Biometric Matching System (BMS) project. This search facility is very important from a law enforcement point of view, since in most cases it is only possible to find latents at a crime scene under investigation.

- **Legal basis**

The Treaty on European Union, and in particular Articles 30(1)(b) and 34(2)(c).

- **Subsidiarity principle**

The subsidiarity principle applies insofar as the proposal does not fall under the exclusive competence of the Community.

The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reason(s).

The proposed actions require an amendment of the EURODAC Regulation in order to add a secondary purpose to it, that of using EURODAC data in the fight against terrorism and crime. This amendment can only be proposed by the Commission. Without this amendment, the Member States have no right to act.

Any action undertaken by Member States alone is likely to be prohibitively expensive and disproportional.

Community action will better achieve the objectives of the proposal for the following reason(s).

The right to consult EURODAC is the simplest, most proportionate and least expensive way to close the identified information gap.

The proposed measures merely permit the request for comparison with EURODAC data. The further cooperation and exchange of information is left to current instruments and to the Member States.

The proposal therefore complies with the subsidiarity principle.

- **Proportionality principle**

The proposal complies with the proportionality principle for the following reason(s).

Access of law enforcement authorities to EURODAC is the only timely, accurate, secure and cost-efficient way to identify whether and if so where data about asylum seekers are available in the Member States. No reasonable efficient alternative exists to EURODAC to establish or verify the exact identity of an asylum seeker that allows law enforcement authorities to obtain the same result. The proposed measures focus on the essentials of the right to consultation, and do not go beyond what is proportionate.

The proposed measure involves the least costs on the Community and the Member States, as it uses existing databases and existing information sharing structures and does not seek to create new such systems.

- **Choice of instruments**

Proposed instruments: other.

Other means would not be adequate for the following reason(s).

Since fundamental rights are at stake, other regulatory means than a Decision under Title VI TEU would not be appropriate.

4. BUDGETARY IMPLICATION

The proposal would entail a technical amendment to EURODAC in order to provide the possibility to carry out a comparison on the basis of a latent.

5. ADDITIONAL INFORMATION

- **Review/revision/sunset clause**

The proposal includes a review clause.

2009/0130 (CNS)

Proposal for a

COUNCIL DECISION

on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30(1)(b) and 34(2)(c) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament[1],

Whereas:

(1) The Hague Program on strengthening freedom, security and justice in the European Union, as adopted by the European Council on 4 November 2004, asked for improvement of the cross-border exchange of data, also by extending the access to existing data filing systems of the European Union.

(2) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in EURODAC established by the Council Regulation (EC) No …/… [*new Eurodac*][2] is necessary for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences. Therefore, the data in EURODAC should be available, subject to the conditions set out in this Decision, for comparison by the designated authorities of Member States and Europol.

(3) The Commission outlined in its Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs[3] of 24 November 2005 that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. In this Communication the Commission also found that the proportionality principle requires that EURODAC be queried for these purposes only once there is an overriding public security concern, that is, if the act committed by the criminal or terrorist to be

---

1 OJ C , , p. .
2 OJ L , , p. .
3 COM(2005) 597, 24.11.2005.

identified is so reprehensible that it justifies querying a database that registers persons with a clean criminal record and it concluded that the threshold for authorities responsible for internal security to query EURODAC must therefore always be significantly higher than the threshold for querying criminal databases.

(4) Moreover, Europol has a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to EURODAC data within the framework of its tasks and in accordance with the Decision establishing the European Police Office (Europol) No (2009/371/JHA) [4].

(5) This Decision complements Regulation (EC) No […/…] *[new EURODAC]*, insofar as it provides for a legal basis under Title VI of the Treaty establishing the European Union to authorise requests for comparison with EURODAC data by Member States authorities and Europol.

(6) Since EURODAC has been established to facilitate the application of the Dublin Regulation, access to EURODAC for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences constitutes a change of the original purpose of EURODAC, which interferes with the right to respect the private life of individuals whose personal data are processed in EURODAC. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.

(7) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The possibility to compare a latent with the fingerprint data which is stored in EURODAC will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.

(8) This Decision lays down the conditions under which requests for comparison of fingerprint data with EURODAC data for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences should be allowed and the necessary safeguards to ensure the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in EURODAC.

(9) It is necessary to designate the competent Member States' authorities as well as the National Central Access Point through which the requests for comparison with EURODAC data are done and to keep a list of the operating units within the designated authorities that are authorised to request such comparison for the specific

[4] OJ L 121, 15.5.2009, p. 37

purposes of the prevention, detection and investigation of terrorist offences as referred to in the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism[5] and of other serious criminal offences as referred to in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States[6].

(10) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and shall be reasoned. The verifying authorities should be responsible for ensuring strict compliance with the conditions for access as established in this Decision. The verifying authorities should then forward the request for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency the verifying authority should process the request immediately and only do the verification afterwards.

(11) For the purposes of protection of personal data, and in particular to exclude mass comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime[7] (Prüm Decision) have returned negative results. Such a specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.

(12) The Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[8] applies to the personal data which are processed pursuant to this Decision.

(13) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin

---

5 OJ L 164, 22.6.2002, p. 3.
6 OJ L 190, 18.7.2002, p. 1.
7 OJ L 210, 6.8.2008, p. 1.
8 OJ L 350, 30.12.2008, p. 60.

Regulation applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Decision.

(14) National competent authorities for the supervision of the processing of personal data should monitor the lawfulness of the processing of personal data by the Member States, and the Joint Supervisory Body set up by the Europol Decision should monitor the lawfulness of data processing activities performed by EUROPOL.

(15) 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[9] and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply to the processing of personal data by the Community institutions and bodies when carrying out their responsibilities in the operational management of EURODAC in the exercise of activities all or part of which fall within the scope of Community law.

(16) The effective application of this Decision should be evaluated at regular intervals.

(17) Since the objectives of this decision, namely the creation of conditions for requests for comparison with data stored in the EURODAC central database by Member States' designated authorities and by Europol cannot be sufficiently achieved by the Member States and can, therefore, by reason of the scale and effects of the action, be only achieved at the level of the European Union, the Council may adopt measures in accordance with the principle of subsidiarity, referred to in Article 2 of the Treaty on European Union and defined in Article 5 of the Treaty establishing the European Community. In accordance with the principle of proportionality as set out in those Articles, this Decision does not go beyond what is necessary in order to achieve those objectives.

(18) In accordance with Article 47 of the Treaty on the European Union, this Decision does not affect the competences of the European Community, in particular as exercised in Regulation (EC) No […/…] *[new EURODAC]*[10] and in 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 movement of such data[11].

(19) This Decision respects the fundamental rights and observes the principles reflected in particular in the Charter of Fundamental Rights of the European Union and notably the right to protection of personal data and the right to asylum. This Decision should be applied in accordance with these rights and principles,

---

9 OJ L 8, 12.1.2001, p. 1.

10 …….

11 OJ L 281, 23.11.1995, p. 31.

HAS ADOPTED THIS DECISION:

CHAPTER I

GENERAL PROVISIONS

Article 1
Subject matter and scope

This Decision lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.

Article 2
Definitions

1. For the purposes of this Decision, the following definitions shall apply:

(a) 'EURODAC' means the database as established by Regulation (EC) No […/…] *[new EURODAC];*

(b) 'Europol' means the European Police Office as established by Council Decision […/…./JHA];

(c) 'EURODAC data' means all fingerprint data stored in the central database in accordance with Article 9 and Article 14(2) of *[new EURODAC];*

(d) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA;

(e) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law;

(f) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent;

(g) 'National Access Point' is the designated national system which communicates with the Central System as referred to in Article 4(2) of the *[new EURODAC];*

(h) Management Authority means the entity responsible for the operational management of EURODAC referred to in Article 5 of the *[new EURODAC]*.

2. The definitions in Regulation (EC) No […/…] *[new EURODAC]* shall also apply.

Article 3
Designated authorities

1. Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Decision. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. Designated authorities shall not include agencies or units dealing especially with national security issues.

2. Every Member State shall keep a list of the designated authorities.

3. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request comparisons with EURODAC data through the National Access Point.

Article 4
Verifying authorities

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. Verifying authorities shall not include agencies or units dealing especially with national security issues.

2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.

3. Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point which communicates with the Central System.

Article 5
Europol

1. Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.

2. EUROPOL shall designate an operating unit that is authorised to request comparisons with EURODAC data through its designated National Access Point.

CHAPTER II

PROCEDURE FOR COMPARISON AND DATA TRANSMISSION

Article 6
Procedure for comparison of fingerprint data with EURODAC data

1. The designated authorities referred to in Article 3(1) and Europol may submit a reasoned electronic request to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 7 or Article 8, as appropriate, are fulfilled.

2. Where all the conditions for requesting a comparison are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the EURODAC Central System for the purpose of comparison with all the EURODAC data.

3. In exceptional cases of urgency, the verifying authority may transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions of Article 7 or Article 8 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.

4. Where the ex-post verification determines that the access was not justified, the information communicated from EURODAC shall be destroyed by all authorities which have accessed it and they shall inform the verifying authority of such destruction.

Article 7
Conditions for access to EURODAC data by designated authorities

1. Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA [12] return negative results and where:

   (a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;

[12] OJ L 210, 6.8.2008, p. 1.

(b) the comparison is necessary in a specific case;

(c) there are reasonable grounds to consider that such comparison with EURODAC data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.

2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.

Article 8
Conditions for access to EURODAC data by Europol

1. Requests for comparison with EURODAC data by Europol shall take place within the limits of its mandate and where necessary for the performance of its tasks pursuant to the Europol Decision and for the purposes of a specific analysis or an analysis of a general nature and of a strategic type.

2. Requests for comparison with EURODAC data shall be limited to comparisons of fingerprint data.

3. Processing of information obtained by Europol from comparison with EURODAC shall be subject to the authorisation of the Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.

Article 9
Communication between the verifying authorities and the National Access Points

1. EURODAC Communication Infrastructure shall be used for the data transmission by the verifying authorities of Member States and Europol to the National Access Points and vice versa . All communications shall take place electronically.

2. Fingerprints shall be digitally processed by the Member State and transmitted in the data format referred to in Annex I to the Regulation (EC) No […/…] *[new EURODAC]*, in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.

CHAPTER III

PERSONAL DATA PROTECTION

Article 10
Protection of personal data

1. The Framework Decision 2008/977/JHA is applicable to the processing of personal data under this Decision.

2. The processing of personal data by Europol pursuant to this Decision shall be in accordance with the [Europol] Decision […/…/JHA] and the rules adopted in implementation thereof and shall be supervised by the independent joint supervisory body established by Article 34 of that Decision.

3. Personal data obtained pursuant to this Decision from EURODAC shall only be processed for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences.

4. Personal data obtained by a Member State or Europol pursuant to this Decision from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol.

5. The monitoring of the lawfulness of the processing of personal data under this Decision by the Member States, including their transmission to and from EURODAC shall be carried out by the national competent authorities designated pursuant to Framework Decision 2008/977/JHA.

Article 11
Data security

1. The Member State responsible shall ensure the security of the data during all transmissions of data under this Decision to the designated authorities and when received by them.

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 processing);

(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 to request comparisons with data held in EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the National Supervisory Authorities designated under Article 25 of the Framework Decision 2008/977/JHA 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 Decision (self-auditing).

Article 12

Prohibition of transfers of data to third countries or to international bodies or to private parties

Personal data obtained by a Member State or Europol pursuant to this Decision from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies, provided that the conditions of Article 13 of the Framework Decision 2008/977/JHA are fulfilled.

Article 13

Logging and documentation

1. Each Member State and Europol shall ensure that all data processing operations resulting from requests for comparison with EURODAC data pursuant to this Decision are logged or documented for the purposes of checking the admissibility of the request monitoring the lawfulness of the data processing and data integrity and security and for self-monitoring.

2. The log or documentation shall show in all cases:

   (a) the exact purpose of the request for comparison, including the concerned form of a terrorist offence or other serious criminal offence and for Europol, the exact purpose of the request for comparison;

   (b) the respective national file reference;

(c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;

(d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;

(e) where applicable the use of the urgent procedure referred to in Article 6(3) and the decision taken with regard to the ex-post verification;

(f) the data used for comparison;

(g) according to national rules or the rules of the Europol Decision the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

3. Such logs or documentation shall be used only for the data protection monitoring of the lawfulness of data processing as well as to ensure data security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 17. The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data processing and data integrity and security, shall have access to these logs at their request for the purpose of fulfilling their duties.

TITLE IV

FINAL PROVISIONS

Article 14
Costs

Each Member State and Europol shall set up and maintain at their expense, the technical infrastructure necessary to implement this Decision, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of this Decision.

Article 15
Penalties

Member States and Europol shall take the necessary measures to ensure that any use of EURODAC data contrary to the provisions of this Decision is punishable by penalties, including administrative and/or criminal penalties, which are effective, proportionate and dissuasive.

Article 16

Notification of designated authorities and verifying authorities

1. By [three months after the date of entry into force of this Decision] at the latest each Member State shall notify the Commission and the General Secretariat of the Council of its designated authorities and shall notify without delay any amendment thereto.

2. By [three months after the date of entry into force of this Decision] at the latest each Member State shall notify the Commission and the General Secretariat of the Council of its verifying authority and shall notify without delay any amendment thereto.

3. By [three months after the date of entry into force of this Decision] at the latest Europol shall notify the Commission and the General Secretariat of the Council of its verifying authority and the National Access Point which it has designated and shall notify without delay any amendment thereto.

4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the *Official Journal of the European Union* on an annual basis.

Article 17

Monitoring and evaluation

1. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.

2. Three years after the entry into force of this Decision and every four years thereafter, the Commission shall produce an overall evaluation of this Decision. This evaluation should include an examination of the results achieved against objectives and an assessment of the continuing validity of the underlying rationale, and shall make any necessary recommendations. The Commission shall submit the evaluation report to the European Parliament and the Council.

3. The Management Authority, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 2. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.

Article 18

Entry into force and date of application

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

2. This Decision shall apply from the date referred to in Article 33(2) of Regulation […] *[new EURODAC]*.

Done at Brussels,

For the Council
The President