



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 4 June 2012**

**10638/12**

**Interinstitutional File:  
2008/0242 (COD)**

**EURODAC 3  
ENFOPOL 157  
CODEC 1503**

**PROPOSAL**

---

from: Secretary-General of the European Commission,  
signed by Mr Jordi AYET PUIGARNAU, Director

dated: 1 June 2012

---

No Cion doc.: COM(2012) 254 final

---

Subject: Amended proposal for a REGULATION OF THE EUROPEAN  
PARLIAMENT AND OF THE COUNCIL on the establishment of  
'EURODAC' for the comparison of fingerprints for the effective application of  
Regulation (EU) 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 to request comparisons with EURODAC  
data by Member States' law enforcement authorities and Europol for law  
enforcement purposes and amending Regulation (EU) No 1077/2011  
establishing a European Agency for the operational management of large-scale  
IT systems in the area of freedom, security and justice (Recast version)

---

Delegations will find attached a proposal from the Commission, submitted under a covering letter from Mr Jordi AYET PUIGARNAU, Director to Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union.

---

Encl.: COM(2012) 254 final

EUROPEAN COMMISSION

Brussels, 30.5.2012  
COM(2012) 254 final

2008/0242 (COD)

Amended proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) 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 to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice**

**(Recast version)**

## EXPLANATORY MEMORANDUM

### 1. CONTEXT OF THE PROPOSAL

EURODAC was established by Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention<sup>1</sup>. A recast proposal for the amendment of the EURODAC Regulation was adopted by the Commission in December 2008<sup>2</sup> (hereafter the December 2008 proposal).

This proposal was designed to ensure a more efficient support to the application of the Dublin Regulation<sup>3</sup> and to properly address data protection concerns. It also aligned the IT management framework to that of the SIS II and VIS Regulations by providing for the taking over of the tasks of the operational management for EURODAC by the future Agency for the operational management of large-scale IT systems in the area of freedom, security and justice<sup>4</sup> (hereafter: IT Agency). The December 2008 proposal also proposed to repeal the Implementing Regulation and to include its content in the EURODAC Regulation. Finally, changes were introduced to take into account developments in the asylum *acquis* and technical progress which took place since the adoption of the Regulation in 2000.

The proposal was sent to European Parliament and the Council on 3 December 2008. The European Parliament referred the proposal to its Committee on Civil Liberties, Justice and Home Affairs (LIBE). At its sitting on 7 May 2009, the European Parliament adopted a legislative resolution<sup>5</sup> endorsing the Commission proposal subject to a number of amendments.

The Commission adopted an amended proposal in September 2009 in order to, on the one hand, take into account the resolution of the European Parliament and the results of negotiations in the Council, and, on the other hand, introduce the possibility for Member States' law enforcement authorities and Europol to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences (the September 2009 proposal).<sup>6</sup>

---

<sup>1</sup> OJ L 062, 05.03.2002, p. 1.

<sup>2</sup> 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], COM(2008)825 final.

<sup>3</sup> Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national. OJ L 50, 25.02.2003, p. 1

<sup>4</sup> The Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [COM(2009) 293 final] was adopted on 24 June 2009. An amended proposal was adopted on 19 March 2010: Amended proposal for a Regulation (EU) No .../... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2010)93.

<sup>5</sup> Establishment of 'Eurodac' for the comparison of fingerprints (recast), P6\_TA(2009)0378.

<sup>6</sup> Such a proposal was called for by Council Conclusions on access to Eurodac by Member States' police and law enforcement authorities as well as Europol of 12 and 13 June 2007.

In particular, that proposal introduced a bridging clause to allow access for law enforcement purposes as well as the necessary accompanying provisions and amended the December 2008 proposal. It was presented at the same time as the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes<sup>1</sup> (hereafter: the Council Decision), spelling out the exact modalities of such access.

The European Parliament did not issue a legislative resolution on the September 2009 proposals.

With the entry into force of the Treaty on the Functioning of the European Union (TFEU) and the abolition of the pillar system, the proposal for a Council Decision lapsed. According to the Communication on the consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures,<sup>2</sup> such proposals would be formally withdrawn and replaced with a new proposal to take account of the new framework of the TFEU.

However, with a view to progressing on the negotiations on the asylum package and facilitating the conclusion of an agreement on the EURODAC Regulation, the Commission considered it more appropriate in 2010 to withdraw from the EURODAC Regulation those provisions referring to the access for law enforcement purposes and presented a new proposal on 11.10.2010<sup>3</sup> similar to the 2008 recast of the EURODAC Regulation.

The Commission noted in the Explanatory Memorandum to its 2010 proposal that enabling the swifter adoption of the new EURODAC Regulation would also facilitate the timely set up of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, since that Agency is to become responsible for the management of EURODAC as from 1 December 2012.

It has since become clear however that including law enforcement access for EURODAC is needed as part of a balanced deal on the negotiations of the Common European Asylum System package with a view to completing the package by the end of 2012. Accordingly the Commission has decided to present again proposals to permit law enforcement access to EURODAC, but on this occasion merged into a single new EURODAC Regulation as this is now possible since the entry into force of the TFEU and it is better legislative practice to present a single instrument.

Regulation (EU) No 1077/2011 of the European Parliament and the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale information systems in the area of freedom, security and justice provides that the Agency should perform the tasks relating to EURODAC conferred on the Commission as the authority responsible for the operational management of EURODAC in accordance with Regulations (EC) No 2725/2000 and (EC) No 407/2002 as well as certain tasks related to the communication infrastructure, namely, supervision, security and the coordination of relations between the Member States and the provider. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should be granted observer status in the Management Board of the Agency when a question concerning EURODAC is on the agenda.

---

<sup>1</sup> COM(2009) 344.

<sup>2</sup> COM(2009) 665 final/2.

<sup>3</sup> COM(2010) 555 final.

The current proposal therefore withdraws the 2010 proposal and replaces it with a new one in order first to take into account the resolution of the European Parliament and the results of negotiations in the Council; second, to introduce the possibility for Member States' law enforcement authorities and Europol to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences; and third, to introduce the necessary amendments to Regulation (EU) No 1077/2011.

The proposal addresses a structural information and verification gap that currently results from the lack of an EU instrument available to law enforcement authorities to determine the Member State that holds information on an asylum seeker. While data on EU citizens exist in many different databases in Member States which are in general accessible to law enforcement authorities in other Member States, there are no effective possibilities available for law enforcement authorities to exchange information on asylum seekers.

The intention is now to allow consultation of EURODAC by law enforcement authorities for the purpose of prevention, detection and investigation of terrorist offences and other serious criminal offences. This aims at enabling law enforcement authorities to request the comparison of fingerprint data with those stored in the EURODAC central database when they seek to establish the exact identity of or get further information on a person who is suspected of a serious crime or a crime victim. Fingerprint data constitute an important element of establishing the exact identity of a person and it is generally acknowledged as an important source of information for prevention, detection and investigation of terrorist offences and other serious criminal offences. On a 'hit'/'no hit' basis, the requesting law enforcement authority will be informed if information on the person is available in the national asylum database of another Member States. In this case, further information on the person can be requested from that Member State by using existing instruments for information exchange, such as Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities.

Comparison of fingerprints in possession of Member States' designated law enforcement authorities and Europol with those stored in the EURODAC database will only be possible in case of necessity of such comparison in a specific case under well-defined circumstances. Provisions on access to data and data security take into account access for law enforcement purposes. It is therefore necessary to amend the EURODAC Regulation to include this additional purpose.

#### General context

The Hague Programme called for the improvement of the cross-border exchange of data by law enforcement authorities, also by extending the access to existing data filing systems of the European Union. The Stockholm Programme called for well targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.

The conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 invited the Commission to present as soon as possible the necessary proposals to achieve the aim of granting access under certain conditions to EURODAC to Member States' law enforcement authorities and Europol, to assist them in the course of their duties in relation to the prevention, detection and investigation of terrorist offences and other serious criminal offences.

The impacts of the access for law enforcement purposes introduced in the present amended proposal are assessed by an Impact Assessment attached to this proposal.

The current proposal also amends Regulation (EU) No 1077/2011 (the Agency Regulation) in order to align it to the present Regulation.

## **2. CONSISTENCY WITH OTHER POLICIES**

This proposal is fully in line with the Hague programme of 2004 and the Stockholm Programme of 2009, the European Pact on Immigration and Asylum endorsed by the European Council of 15-16 October 2008 and the Charter of Fundamental Rights of the European Union, in particular as regards the right to asylum and protection of personal data.

Furthermore, this proposal is in line with the Commission's 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<sup>1</sup>, which noted that the Council and the law enforcement community identify the absence of access by internal security authorities to VIS, SIS II immigration and EURODAC data as a shortcoming, which results in a serious gap in the identification of suspected perpetrators of terrorist or serious crimes. Since the adoption of the Communication in 2005, the VIS Decision was adopted in order to grant law enforcement authorities and Europol access to that database.

## **3. COMPLIANCE WITH THE CHARTER OF FUNDAMENTAL RIGHTS**

The respect for fundamental rights is a legal requirement subject to the scrutiny of the European Court of Justice. The institutions, bodies, agencies and offices of the European Union and its Member States when implementing European Union law are bound by the EU Charter of Fundamental Rights which has the same legal value as the Treaties. Respect of fundamental rights is a condition of the lawfulness of EU acts. During the drafting exercise, full account was taken of the impacts on fundamental rights in order to ensure that the proposal complies with the fundamental rights protected by the Charter. Due attention to the right to asylum and the right to the protection of personal data was thoroughly considered in the Impact Assessment attached to the proposal.<sup>2</sup>

As regards the right to asylum, guaranteed by Article 18 of the Charter, amendments to the provisions of the Regulation on the information to be given to asylum seekers on the application of the Dublin system enables them to effectively exercise their right to asylum. The new provision that requires Member States to indicate in EURODAC the fact that they apply the discretionary clauses of the Dublin Regulation, facilitates communication amongst Member States and therefore prevents uncertainty for the asylum seeker, by making clarity about which Member State handles his case. 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

<sup>1</sup> COM(2005) 597.

<sup>2</sup> See pages 15-16 and 57 of the 2009 Impact Assessment SEC(2009) 936.

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 search functionality for law enforcement purposes will have led to the stigmatisation of persons seeking international protection. Consequently, the proposal does not limit the right to asylum as guaranteed by Article 18 of the Charter.

As regards the right to the protection of personal data guaranteed by Article 8 of the Charter, by allowing for efficient management of erasure of data, the proposal ensures that no data should be kept in a form which allows the identification of data subjects for longer than is necessary for the purposes for which data were collected. The same principle underpins the amendment aligning the storage period for data on third country nationals or stateless persons fingerprinted in connection with the irregular crossing of an external border with the period until which the Dublin Regulation allocates responsibility on the basis of that information.

The comparison with EURODAC data for the prevention, detection or investigation of terrorist offences or other serious criminal offences constitutes a limitation of the right to the protection of personal data, as these purposes are not compatible with the purposes for which the data were originally collected and for which EURODAC has been established. Moreover, EURODAC contains data of individuals who in principle are not suspected of committing any crime.

The use of EURODAC data for law enforcement purposes implies a change of purpose of the data processed and constitutes an "interference" with the right to data protection<sup>1</sup>. As stipulated by Article 52(1) of the Charter, any limitation to the right to the protection of personal data must be provided for by law, must respect the essence of the right, must be necessary to achieve an objective of general interest recognised by the Union or to protect the rights and freedoms of others, and must be proportionate, i.e. appropriate for attaining the objective pursued and not going beyond what is necessary to achieve it.

The law imposing such a limitation must be formulated with sufficient precision to allow individuals to adjust their conduct and protect them against arbitrariness. It must also indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise<sup>2</sup>. The prevention, detection or investigation of terrorist offences or other serious criminal offences contributes to the establishment of an area of freedom, security and justice as a general interest recognised by the Union in Article 3(2) TFEU. Article 8(2) of the European Convention of Human Rights also recognises that interference by a public authority with a person's right to privacy may be justified as necessary in the interest of national security, public safety or the prevention of crime. The proposal provides for a more effective and less intrusive measure for competent law enforcement authorities to determine if another Member State holds data on an asylum seeker. Under current rules, Member States' law enforcement authorities have to contact bilaterally all other Member States participating in EURODAC to determine if another Member State holds data on an asylum seeker. This inefficient crime resolution under the current rules requires that law enforcement authorities access more personal data or data on more persons than is necessary to establish whether relevant information exists.

---

<sup>1</sup> See the reference to "interference" in Judgment of the ECJ of 20 May 2003, *Österreichischer Rundfunk and Others*. Joined Cases C-465/2000, C-138/01 and C-139/01, ECR [2003], p. I-4989, paragraph 83

<sup>2</sup> Joined applications 30562/04 and 30566/04, *S. and Marper v. United Kingdom*, judgment of 4 December 2008.

Indeed, the proposal provides for effective safeguards that mitigate the limitation of the right to the protection of personal data. The comparison of EURODAC data for law enforcement purposes follows a two-step approach, as this comparison may only be made after a prior Prüm check under Council Decision 2008/615/JHA and if the Prüm check returns negative results. This means that Member States that have not implemented Council Decision 2008/615/JHA will not be able to conduct searches in EURODAC for law enforcement purposes.

Moreover, the comparison of EURODAC data for law enforcement purposes may only be made for the prevention, detection or investigation of terrorist offences or other serious criminal offences if it is necessary in a specific case as they are defined in Council Framework Decisions 2002/475/JHA on combating terrorism and 2002/584/JHA on the European arrest warrant. This excludes both the comparison of EURODAC data for the crimes that are not serious and a systematic or mass comparison of data. Moreover, designated law enforcement authorities may only request the comparison with EURODAC data if there are reasonable grounds to consider that such comparison will substantially contribute to the prevention, detection or investigation of the criminal offence in question. Upon receipt of such request by a designated law enforcement authority, a verifying authority verifies whether the strict conditions for requesting a comparison with EURODAC data for law enforcement purposes are fulfilled. If the verifying authority agrees with the request, it will transmit the request to the National Access Point which will process it to the EURODAC Central System. Member States may not conduct searches on a systematic and routine basis. Thus, as an additional safeguard, the proposal provides for a three-step approach in relation to the authorities that can consult the EURODAC system. The comparison with EURODAC for law enforcement purposes will provide a result on a 'hit'/'no hit' basis, i.e. it will only determine if another Member State holds data on an asylum seeker. The proposal does not provide for new possibilities to process additional personal information in the follow-up to a 'hit'.

Furthermore, the proposal also lays down strict data security measures to ensure the security of personal data processed and establishes supervision of the processing activities by independent public data protection authorities and documentation of all searches conducted. The proposal also states that the processing of all personal data carried out by law enforcement authorities on EURODAC data once they have been extracted is subject to Council Framework Decision 2008/977/JHA.

Individuals should be given rights of access, correction and redress in particular the right to a judicial remedy, and supervision of processing operations by public independent authorities should be ensured. The European Data Protection Supervisor (as regards all processing activities in EURODAC) and national data protection authorities will supervise the compliance with data protection law and if appropriate will enforce it. Consequently, the limitation of the right to the protection of personal data by the comparison with EURODAC data as provided by this proposal is surrounded with the necessary safeguards to ensure the respect of the fundamental rights.

Databases of asylum seekers might contain fingerprint data from persons as young as 14 years, but children of this age are not criminally responsible in all Member States. Member States have to ensure that the data of children they retrieve by consulting such databases and which, according to their national law, cannot be held criminally responsible, are treated in a legal and non-discriminatory manner (in comparison with the data from children who are



citizens of the concerned Member State) while respecting the principle of the best interests of the child.

Therefore, this proposal fully complies with the Charter of Fundamental Rights of the European Union, in particular as regards the right to asylum (Article 18) and protection of personal data (Article 8). The proposal is also in line with Article 16 TFEU, which guarantees everyone the right to the protection of personal data.

#### **4. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENTS**

The present amended proposal reinstates all of the provisions proposed in the lapsed draft Council Decision of 2009. In addition, it introduces two technical provisions relating to the asylum provisions.<sup>1</sup> None of these elements is new and all were explored thoroughly in the Impact Assessments to the previous 2008 and 2009 proposals. Therefore, no new consultation and impact assessment were conducted specifically for the present proposal. However, the Impact Assessments of 2008 and 2009<sup>2</sup> are still valid for its purposes.

The Commission published the Green Paper on the future Common European Asylum System<sup>3</sup> in June 2007, which proposed options concerning the future features of the Dublin and EURODAC Regulations. In the framework of the wide public consultation on the Green Paper, 89 contributions were received from a wide range of stakeholders.

The Commission services discussed the outcome of the Evaluation Report and the outline of the planned amendments to the Regulation with the Member States in the Committee on Immigration and Asylum (CIA) in March 2008 as well as in two informal expert meetings with Member States' practitioners dedicated to the conclusions of the Evaluation Report in October 2007 and April 2008.

UNHCR, the European Council on Refugees and Exiles (ECRE) as well as the European Data Protection Supervisor (EDPS) were also informally consulted in the preparation of the amendment of the Regulation.

During the drafting of the 2008 proposals concerning improvements to the functioning of EURODAC and to the 2009 amended proposals relating to law enforcement access, 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. Several intergovernmental organisations, non-governmental organisations and other experts working in the area of asylum, fundamental rights were consulted during a meeting in Brussels on 8 October 2007. 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 were consulted in the framework of a meeting held in Brussels on 11 October 2007. As Liechtenstein has only applied the Dublin *acquis* very recently, there has not been an opportunity to consult Liechtenstein on this proposal.

---

<sup>1</sup> One to ensure consistency with the Dublin Regulation and one to clarify the need for having the system's automated hit replies verified by a fingerprints expert.

<sup>2</sup> SEC(2008) 2981 and SEC(2009) 936

<sup>3</sup> COM(2007) 301.

A detailed list of consulted parties was included in the Impact Assessment attached to the 2009 proposal.

## 5. LEGAL ELEMENTS OF THE PROPOSAL

This proposal amends the 2010 Amended proposal for a Commission 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] - COM(2010) 555.

This proposal also amends Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

The present amended proposal uses Article 78(2)(e) of the Treaty on the Functioning of the European Union (TFEU) as legal base concerning criteria and mechanisms for determining which Member State is responsible for considering an application for asylum or subsidiary protection, which is the TFEU Article corresponding to the legal base of the original proposal (Article 63(1)(a) of the Treaty establishing the European Community). In addition, it uses Article 87(2)(a) as the legal base concerning the elements related to the collation, storage, processing, analysis and exchange of relevant information for law enforcement purposes; and Article 88(2)(a) as the legal base concerning Europol's field of action and tasks including the collection, storage, processing, analysis and exchange of information.

Title V of the TFEU is not applicable to the United Kingdom and Ireland, unless those two countries decide otherwise, in accordance with the provisions set out in the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on the European Union (TEU) and to the TFEU.

The United Kingdom and Ireland are bound by Council Regulation (EC) No 2725/2000 following their notice of their wish to take part in the adoption and application of that Regulation based on the above-mentioned Protocol. The position of these Member States with regard to the current Regulation does not affect their possible participation with regard to the amended Regulation.

Under the Protocol on the position of Denmark, annexed to the TEU and the TFEU, Denmark does not take part in the adoption by the Council of the measures pursuant to Title V of the TFEU (with the exception of "measures determining the third countries whose nationals must be in possession of a visa when crossing the external borders of the Member States, or measures relating to a uniform format for visas"). Therefore, Denmark does not take part in the adoption of this Regulation and is not bound by it nor subject to its application. However, given that Denmark applies the current Eurodac Regulation, following an international agreement<sup>1</sup> that it concluded with the EC in 2006, it shall, in accordance with Article 3 of that agreement, notify the Commission of its decision whether or not to implement the content of the amended Regulation.

---

<sup>1</sup> Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention (OJ L 66, 8.3.2006).

This proposal maintains the changes made in the previous proposals to abolish the Committee provided for in Article 22 of the Regulation.

## **6. IMPACT OF THE PROPOSAL ON NON-EU MEMBER STATES ASSOCIATED TO THE DUBLIN SYSTEM**

In parallel to the association of several non-EU Member States to the Schengen *acquis*, the Community concluded, or is in the process of doing so, several agreements associating these countries also to the Dublin/EURODAC *acquis*:

- the agreement associating Iceland and Norway, concluded in 2001<sup>1</sup>;
- the agreement associating Switzerland, concluded on 28 February 2008<sup>2</sup>;
- the protocol associating Liechtenstein, concluded on 18 June 2011<sup>3</sup>.

In order to create rights and obligations between Denmark – which as explained above has been associated to the Dublin/EURODAC *acquis* via an international agreement – and the associated countries mentioned above, two other instruments have been concluded between the Community and the associated countries.<sup>4</sup>

In accordance with the three above-cited agreements, the associated countries shall accept the Dublin/EURODAC *acquis* and its development without exception. They do not take part in the adoption of any acts amending or building upon the Dublin *acquis* (including therefore this proposal) but have to notify to the Commission within a given time-frame of their decision whether or not to accept the content of that act, once approved by the Council and the European Parliament. In case Norway, Iceland, Switzerland or Liechtenstein do not accept an act amending or building upon the Dublin/EURODAC *acquis*, the "guillotine" clause is applied and the respective agreements will be terminated, unless the Joint/Mixed Committee established by the agreements decides otherwise by unanimity.

The scope of the above-cited association agreements with Iceland, Norway, Switzerland and Liechtenstein as well as the parallel agreement with Denmark does not cover law enforcement access to EURODAC.

---

<sup>1</sup> Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway (OJ L 93, 3.4.2001, p. 40).

<sup>2</sup> Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland (OJ L 53, 27.2.2008, p. 5).

<sup>3</sup> Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland (OJ L 160 18.6.2011 p. 39)

<sup>4</sup> Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland (2006/0257 CNS, concluded on 24.10.2008, publication in OJ pending) and Protocol to the Agreement between the Community, Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State, Iceland and Norway (OJ L 93, 3.4.2001).

The current proposal, as per the 2009 proposal, notes that the comparison of fingerprint data using EURODAC may only be made after national fingerprint databases and the Automated Fingerprint Databases of other Member States under Council Decision 2008/615/JHA (the Prüm Agreements) return negative results. This rule means that if any Member State has not implemented the above Council Decision and cannot perform a Prüm check, it also may not make a EURODAC check for law enforcement purposes. Similarly, any associated States that have not implemented or do not participate in the Prüm Agreements may not conduct such a EURODAC check.

## **7. DETAILED EXPLANATION OF THE PROPOSAL**

References to the "blocking" of data were changed in the 2008 recast to the "marking" of data concerning recognised beneficiaries of international protection. Under the original Regulation, the data of persons granted international protection remained on the EURODAC system but were blocked. As such, the EURODAC system recorded when there were hits concerning the fingerprints of recognised beneficiaries of international protection, but Member States were not informed of these hits. The new proposal was designed to "mark" these data instead in order to inform the Member States if there is a hit for a marked data subject. This is to inform Member States if an existing beneficiary of international protection attempts to put in a fresh claim for asylum.

Several of the amendments to the 2010 proposal are extracted directly from the lapsed September 2009 proposal on law enforcement access to EURODAC. As such, this section has been split into those areas amending the remainder of the proposal and amendments that are largely inspired by the September 2009 proposal, including their article references for ease of comparison.

### **The elements incorporated from the September 2009 proposal are the following.**

Articles 1(2) laying down the conditions – from Article 1 of the September 2009 proposal.

Article 5 on designated authorised to access EURODAC data – from Article 3 of the September 2009 proposal, except for clarified title.

Article 6 on verifying authorities whose purpose is to ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled – from Article 4 of the September 2009 proposal.

Article 7 on Europol – from Article 5 of the September 2009 proposal.

Chapter VI (Articles 19-22) on the procedure for comparison and data transmission for law enforcement purposes – from Articles 6-9 of the September 2009 proposal.

Article 33 on data protection, 34 on data security, 35 on prohibition of data transfers, 36 on logging and transfers – from Articles 10-13 of the September 2009 proposal.

Article 39(3) on costs related to the prevention, detection or investigation of any of the criminal offences defined in this Regulation – from Article 14 of the September 2009 proposal.

Article 40(8) and (9) on annual reporting on law enforcement access to EURODAC – modified from Article 17(1) and 17(3) of the September 2009 proposal.

Article 43 on notification of designated and verifying authorities – from Article 16 of the September 2009 proposal.

**The elements that were neither in the September 2009 proposal nor the 2010 proposal are the following:**

Article 2(1) contains further definitions concerning the IT Agency and Europol and the nature of terrorist and criminal offences.

Article 2(2) and 2(4) clarify for data protection purposes when Directive 95/46/EC and how Framework Decision 2008/977/JHA apply.

Article 29 – the wording on the leaflet has been enhanced to ensure that it is simple and written in a language the applicant can understand.

Chapter VIII (Article 38) makes several amendments to Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. Article 41 – the words "and Europol" have been included into the article on penalties.

Throughout the recast, the references to the "Management Authority" have been replaced with the "Agency".

## **8. BUDGETARY IMPLICATION**

The present proposal entails a technical amendment to the EURODAC central system in order to provide for the possibility to carry out comparisons for law enforcement purposes. A new functionality to search on the basis of a latent is also proposed.

This proposal retains from the 2010 proposal the improvements of the system as regards new, asylum-focused functionalities regarding information on the status of the data subject (which were the outcome of negotiations in the Council). The financial statement attached to this proposal reflects this change and is also valid for the elements concerning the request for comparison with EURODAC data by Member States' law enforcement authorities and by Europol for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences - COM(2009) 344.

The non-administrative cost estimate of 2,415 million EUR (2,771 million EUR including administrative / human resources costs) includes costs of 3 years of technical maintenance, and consists of IT-related services, software and hardware and would cover the upgrade and customisation to allow searches for law enforcement purposes and also the changes for the original asylum purpose unrelated to law enforcement access. The amounts of the EURODAC recast proposal adopted on 10 September 2009 have largely been reproduced in the present financial statement and only altered slightly to reflect the staffing costs in the IT Agency. Given the relatively small overall cost, no extra resources and no rectification of the Home Affairs budget will be sought and funding will be found from within existing budget lines, either of the IT Agency or from the Home Affairs budget.

## **9. SUBSIDIARITY PRINCIPLE**

Due to the transnational nature of the problems related to asylum and refugee protection, the EU is well placed to propose solutions in the framework of the Common European Asylum System (CEAS) to the issues described above as problems regarding the EURODAC Regulation. Although an important level of harmonization was reached in the Regulation adopted in 2000, there is still room for developing the support that EURODAC provides to the implementation of the Dublin Regulation. The need for EU action regarding the management of an EU database which was created for assisting in the implementation of a Regulation dealing with transnational movements of asylum seekers seems clear.

An amendment of the EURODAC Regulation is also required in order to add a secondary purpose thereto, namely allow access for the purpose to fight against terrorism and crime to data stored in the EURODAC central database. This objective cannot be sufficiently achieved by the Member States, since such amendment can only be proposed by the Commission.

## **10. PROPORTIONALITY PRINCIPLE**

The impact assessments published along with the 2008 and 2009 proposals<sup>1</sup> assessed each sub-option regarding the problems identified so as to represent an ideal proportion between practical value and efforts needed. It concluded that opting for EU action does not go beyond what is necessary to achieve the objective of solving those problems.

The relevant Impact Assessment concluded that 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 to EURODAC exists to establish or verify the exact identity of an asylum seeker that allows law enforcement authorities to obtain the same result.

---

<sup>1</sup> SEC(2008) 2981 and SEC(2009) 936

↓ 2725/2000/EC (adapted)

⇒ new

2008/0242 (COD)

Amended proposal for a

## REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) 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 to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice**

(Recast version)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union ~~establishing the European Community~~, and in particular Article 78 point (2)(e) ~~63 point (1)(a)~~ ⇒ , Article 87 point (2)(a) and Article 88 point (2)(a) ⇐ thereof,

Having regard to the proposal from the Commission<sup>1</sup>,

Having regard to the opinion of the European Data Protection Supervisor<sup>2</sup>,

~~Having regard to the opinion of the European Parliament<sup>3</sup>~~

⊗ Acting in accordance with the ordinary legislative procedure, ⊗

Whereas:

<sup>1</sup> COM(2012) XXX.

<sup>2</sup> OJ L 92 10.04.2010, p. 1

<sup>3</sup> ~~OJ C 189, 7.7.2000, p. 105 and p. 227 and opinion delivered on 21 September 2000 (not yet published in the Official Journal).~~

---

↓ new

- (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<sup>1</sup> 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<sup>2</sup>. In the interest of clarity, those Regulations should be recast.

---

↓ 2725/2000/EC recital 1

- ~~(1) Member States have ratified the Geneva Convention of 28 July 1951, as amended by the New York Protocol of 31 January 1967, relating to the Status of Refugees.~~

---

↓ 2725/2000/EC recital 2 (adapted)

- ~~(2) Member States have concluded the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed in Dublin on 15 June 1990 (hereinafter referred to as "the Dublin Convention").~~

---

↓ new

- (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, forced by circumstances, legitimately seek international protection in the Union.
- (3) 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. The European Pact on Immigration and Asylum endorsed by the European Council of 15-16 October 2008 called for the completion of the establishment of a Common European Asylum System by creating a single asylum procedure comprising common guarantees and a uniform status for refugees and the beneficiaries of subsidiary protection.

---

<sup>1</sup> OJ L 316, 15.12.2000, p. 1.

<sup>2</sup> OJ L 62, 5.3.2002, p. 1.



---

↓ 2725/2000/EC recital 3 (adapted)  
⇒ new

- (4) For the purposes of applying ~~the Dublin Convention~~  Council Regulation (EU) 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]<sup>1</sup>, it is necessary to establish the identity of applicants for ~~asylum~~ ⇒ international protection ⇐ and of persons apprehended in connection with the unlawful crossing of the external borders of the Community. It is also desirable, in order effectively to apply the ~~Dublin Convention~~  Council Regulation (EU) 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 ~~(c) and (e)~~ (b) and (d) of Article ~~10(1)~~18(1) thereof, to allow each Member State to check whether an ~~alien~~  third country national or stateless person  found illegally present  staying  on its territory has applied for ~~asylum~~ ⇒ international protection ⇐ in another Member State.
- 

↓ 2725/2000/EC recital 4

- (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.
- 

↓ 2725/2000/EC recital 5  
⇒ new

- (6) To this end, it is necessary to set up a system known as "~~Eurodac~~EURODAC", consisting of a Central ~~Unit~~ ⇒ System ⇐, ~~to be established within the Commission and~~ 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 database~~ ⇒ Central System, hereinafter the "Communication Infrastructure". ⇐
- 

↓ new

- (7) The Hague Programme called for the improvement of access to existing data filing systems in the European Union. In addition, The Stockholm Programme called for well targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.
- (8) 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 is necessary for the purposes of

---

<sup>1</sup> COM(2008)XXX.

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 Regulation, for comparison by the designated authorities of Member States and Europol.

- (9) 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<sup>1</sup> 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 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.
- (10) 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).<sup>2</sup>
- (11) Since EURODAC has been established to facilitate the application of Council Regulation (EU) 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], 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.
- (12) 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.

---

<sup>1</sup> COM(2005) 597, 24.11.2005.

<sup>2</sup> OJ L 121, 15.5.2009, p. 37

(13) This Regulation also 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.

(14) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with current Union 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<sup>1</sup> and Regulation (EU) 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 to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

↓ 2725/2000/EC recital 6 (adapted)  
⇒ new

(15) It is also necessary to require the Member States promptly to take ⇒ and transmit ⇐ fingerprints ⇒ data ⇐ of every applicant for asylum ⇒ international protection ⇐ and of every alien ⊗ 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.

↓ 2725/2000/EC recital 7 (adapted)  
⇒ new

(16) It is necessary to lay down precise rules on the transmission of such fingerprint data to the Central Unit ⇒ System ⇐, the recording of such fingerprint data and other relevant data in the Central Unit ⇒ System ⇐, their storage, their comparison with other fingerprint data, the transmission of the results of such comparison and the blocking ⇒ 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 aliens ⊗ third country nationals or stateless persons ⊗.

↓ new

(17) Hits obtained from EURODAC should be verified by a fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an

<sup>1</sup> OJ L 304, 30.9.2004, p. 12.

application for international protection lodged in one of the Member States by a third-country national or a stateless person].

↓ 2725/2000/EC recital 8 (adapted)  
⇒ new

- (18) Aliens ⊗ Third country nationals or stateless persons ⊗ who have requested asylum ⇒ international protection ⇐ in one Member State may have the option of requesting asylum ⇒ 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 Unit ⇒ System ⇐ should be of considerable length. Given that most aliens ⊗ third country nationals or stateless persons ⊗ who have stayed in the Community ⊗ European Union ⊗ 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 conservation of fingerprint data.

↓ 2725/2000/EC recital 9 (adapted)

- (19) The conservation 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 aliens ⊗ third country nationals or stateless persons ⊗ obtain citizenship of a Member State.

↓ new

- (20) It is appropriate to store data relating to those data subjects whose fingerprints were initially recorded in EURODAC upon lodging their applications for international protection and who have been granted international protection in a Member State in order to allow data recorded upon lodging an application for international protection to be compared against them.

- (21) The European Agency for the operational management of large-scale information systems in the area of freedom security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011<sup>1</sup> (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of EURODAC in accordance with this Regulation and with certain tasks relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should have observer status at the meetings of the Management Board of the Agency, when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of the Agency.

<sup>1</sup> OJ L 286, 1.11.2011, p. 1.

(22) The Staff Regulations of Officials of the European Union (Staff Regulations of Officials) and the Conditions of Employment of Other Servants of the European Union (Conditions of Employment), laid down in Regulation (EEC, Euratom, ECSC) No 259/68 (15) (together referred to as the ‘Staff Regulations’), should apply to all staff working in the Agency on matters pertaining to this Regulation.

↓ 2725/2000/EC recital 10 (adapted)  
⇒ new

(23) It is necessary to lay down clearly the respective responsibilities of the Commission ⇒ and the Agency ⇐, in respect of the Central Unit ⇐ ⇒ System ⇐ ⇒ and the Communication Infrastructure ⇐, and of the Member States, as regards data ~~use~~ processing, data security, access to, and correction of, recorded data.

↓ new

(24) 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 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<sup>1</sup> 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<sup>2</sup>.

(25) 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 operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying authorities should be responsible for ensuring strict compliance with the conditions for access as established in this Regulation. 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 where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.

(26) For the purposes of protection of personal data, and to exclude systematic 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

<sup>1</sup> OJ L 164, 22.6.2002, p. 3.

<sup>2</sup> OJ L 190, 18.7.2002, p. 1.

and cross-border crime<sup>1</sup> have returned negative results. This condition requires prior implementation of the Council Decision as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. 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.

- (27) In case the requesting Member State establishes that EURODAC data pertains to a minor, these data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws for minors and in accordance with the obligation to give primary consideration to the child's best interest.

---

↓ 2725/2000/EC recital 11

- (28) While the non-contractual liability of the Community in connection with the operation of the ~~Eurodac~~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.

---

↓ 2725/2000/EC recital 12

- (29) In accordance with the principle of subsidiarity as set out in Article 5 of the Treaty, the objective of the proposed measures, namely the creation ~~within the Commission~~ of a system for the comparison of fingerprint data to assist the implementation of the Community's asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved by the Community. In accordance with the principle of proportionality as set out in the said Article, this Regulation does not go beyond what is necessary to achieve ~~that those~~ objectives.

---

↓ 2725/2000/EC recital 15 (adapted)

⇒ new

- (30) 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<sup>2</sup> applies to the processing of personal data by the Member States

---

<sup>1</sup> OJ L 210, 6.8.2008, p. 1.

<sup>2</sup> OJ L 281, 23.11.1995, p. 31.

⊗ carried out in application of this Regulation ~~⊗ within the framework of the Eurodac system~~ → unless such processing takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences ↵.

---

↓ new

(31) Council 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<sup>1</sup> applies to all processing of personal data by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.

---

↓ 2725/2000/EC recital 16

~~(16) By virtue of Article 286 of the Treaty, Directive 95/46/EC also applies to Community institutions and bodies. Since the Central Unit will be established within the Commission, that Directive will apply to the processing of personal data by that Unit.~~

---

↓ 2725/2000/EC recital 17

(32) 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.

---

↓ new

(33) 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 Regulation (EU) 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] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

(34) 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 supervisory authority set up by the Europol Decision should monitor the lawfulness of data processing activities performed by Europol.

---

<sup>1</sup> OJ L 350, 30.12.2008, p. 60.

(35) 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<sup>2</sup> and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply to the processing of personal data by Union institutions, bodies, offices and agencies carried out in application of 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.

(36) It is appropriate that national supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor, as referred to in Article 41 of Regulation (EC) No 45/2001, should monitor the activities of the Union institutions, bodies, offices and agencies in relation to the processing of personal data carried out in application of this Regulation.

---

↓ 2725/2000/EC recital 18  
⇒ new

(37) It is appropriate to monitor and evaluate the performance of ~~Eurodac~~EURODAC ⇒ at regular intervals ⇐.

---

↓ 2725/2000/EC recital 19 (adapted)  
⇒ new

(38) Member States should provide for a system of ~~effective, proportionate and dissuasive~~ penalties to sanction the processing use of data ~~entered~~ in the ~~central database~~ ⇒ Central System ⇐ contrary to the purpose of ~~Eurodac~~EURODAC.

---

↓ new

(39) It is necessary that Member States are informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) 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].

(40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation fully respects the individual's right to protection of his or her personal data and the right to asylum.

(41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to

---

<sup>2</sup> OJ L 8, 12.1.2001, p. 1.



its application. As regards Denmark, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes amendment to the EURODAC Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention<sup>1</sup>. Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union. Once this Recast Regulation is adopted *and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, Denmark will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering* the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.

- (42) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, the United Kingdom *[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation]*.
- (43) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland *[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation]*.
- (44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway<sup>2</sup>. Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in their relations with the Member States of the European Union. Once this Recast Regulation is adopted *and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Republic of Iceland and the Kingdom of Norway will be consulted as to whether they wish to enter into negotiations on complementary agreements also covering* the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.

<sup>1</sup> OJ L 66, 8.3.2006, p. 38.

<sup>2</sup> OJ L 93, 3.4.2001, p. 40.

(45) As regards the Swiss Confederation, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland<sup>1</sup>. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted *and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Swiss Confederation will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering* the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on the application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.

(46) As regards the Principality of Liechtenstein, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland<sup>2</sup>. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted *and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Principality of Liechtenstein will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering* the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on their application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.

---

↓ 2725/2000/EC recital 22 (adapted)

(47) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of ~~the Dublin Convention~~  Regulation (EU) 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] .

---

<sup>1</sup> OJ L 53, 27.2.2008, p. 5

<sup>2</sup> OJ L 160, 18.6.2011, p. 39.

HAVE ADOPTED THIS REGULATION:

## CHAPTER I

### GENERAL PROVISIONS

#### Article 1

#### Purpose of "~~Eurodac~~EURODAC"

1. A system known as "~~Eurodac~~EURODAC" is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to ~~the Dublin Convention~~  Regulation (EU) 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 ~~asylum~~  international protection  lodged in a Member State  by a third country national or a stateless person , and otherwise to facilitate the application of the ~~Dublin Convention~~  Regulation  under the conditions set out in this Regulation.
2. ~~Eurodac shall consist of:~~
  - (a) ~~the Central Unit referred to in Article 3;~~
  - (b) ~~a computerised central database in which the data referred to in Article 5(1), Article 8(2) and Article 11(2) are processed for the purpose of comparing the fingerprint data of applicants for asylum and of the categories of aliens referred to in Article 8(1) and Article 11(1);~~
  - (c) ~~means of data transmission between the Member States and the central database.~~
2. This Regulation also 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.
3. Without prejudice to the processing use of data intended for EurodacEURODAC by the Member State of origin in databases set up under the latter's national law, fingerprint data and

other personal data may be processed in ~~Eurodac~~EURODAC only for the purposes set out in  
⇒ this Regulation and ⇐ Article ~~15(1)~~32(1) of the Dublin ~~Convention~~ Regulation ⇐ .

---

↓ 2725/2000/EC (adapted)  
⇒ new

## Article 2 Definitions

1. For the purposes of this Regulation:

- (a) "the Dublin ~~Convention~~ Regulation ⇐ " means the ~~Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed at Dublin on 15 June 1990~~ Regulation (EU) 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 ~~asylum~~ ⇐ international protection ⇐" means an ~~alien~~ ⇐ third-country national or a stateless person ⇐ who has made an application for ~~asylum or on whose behalf such an application has been made~~ ⇐ international protection as defined in Article 2(g) of Council Directive 2004/83/EC in respect of which a final decision has not yet been taken ⇐;
- (c) "Member State of origin" means:
- (i) in relation to an ~~applicant for asylum~~ ⇐ person covered by Article 6 ⇐, the Member State which transmits the personal data to the Central ~~Unit~~ ⇐ System ⇐ and receives the results of the comparison;
  - (ii) in relation to a person covered by Article ~~8~~ 11, the Member State which transmits the personal data to the Central ~~Unit~~ ⇐ System ⇐;
  - (iii) in relation to a person covered by Article ~~11~~ 14, the Member State which transmits such data to the Central ~~Unit~~ ⇐ System ⇐ and receives the results of the comparison;

↓ 2725/2000/EC (adapted)  
⇒ new

- (d) "~~refugee~~" ⇐ "person granted international protection" ⇐ means a ⇐ third country national or a stateless ⇐ person who has been recognised as a ~~refugee in accordance with the Geneva Convention on Refugees of 28 July 1951, as amended by the New York~~

~~Protocol of 31 January 1967~~ ⇒ entitled to international protection as defined in point (a) of Article 2 of Council Directive 2004/83/EC ⇐;

- (e) "hit" shall mean the existence of a match or matches established by the Central ~~Unit~~ ⇒ System ⇐ by comparison between fingerprint data recorded in the ~~database~~ ⇐ central 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 ~~4(6)~~ 18(4);

---

↓ new

- (f) "National Access Point" means the designated national system which communicates with the Central System;
- (g) "Agency" means the Agency established by Regulation (EU) No 1077/2011;
- (h) 'Europol' means the European Police Office as established by Decision 2009/371/JHA;
- (i) 'EURODAC data' means all fingerprint data stored in the central database in accordance with Article 11 and Article 16(2);
- (j) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA;
- (k) '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;
- (l) '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.

---

↓ 2725/2000/EC (adapted)  
⇒ new

2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation ⇒ unless the processing of personal data takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences ⇐.
3. Unless stated otherwise, the terms defined in Article ~~1~~ 2 of the Dublin ~~Convention~~ ⇐ Regulation ⇐ shall have the same meaning in this Regulation.

---

↓ new

4. The terms defined in Article 2 of the Framework Decision 2008/977/JHA shall have the same meaning in this Regulation in so far as personal data are processed by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.

---

↓ 2725/2000/EC (adapted)

### Article 3

#### ~~Central Unit~~ System architecture and basic principles

- ~~1. A Central Unit shall be established within the Commission which shall be responsible for operating the central database referred to in Article 1(2)(b) on behalf of the Member States. The Central Unit shall be equipped with a computerised fingerprint recognition system.~~

---

↓ new

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 National Access Point.

---

↓ 2725/2000/EC (adapted)  
⇒ new

- ~~2.3.~~ Data on ~~applicants for asylum, persons covered by Articles 8 and persons covered by Article 11~~ 9, 14 and 17 which are processed in the Central ~~Unit~~  ~~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 .

---

↓ 2725/2000/EC Article 1(2) third subparagraph  
⇒ new

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

↓ 2725/2000/EC Article 4(1) second sentence  
⇒ new

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** ⇐ ~~the European Convention on Human Rights and~~ in the United Nations Convention on the Rights of the Child.
- 

↓ new

*Article 4*  
**Operational management**

1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central System.
2. The Agency 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. Before the Agency takes up its responsibilities, the Commission shall be responsible for all tasks attributed to the Agency by this Regulation.
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 interrogation of the Central System.
6. Without prejudice to Article 17 of Regulation No 31 (EEC), 11 (EAEC)<sup>1</sup>, the Agency 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.

---

↓ new

#### *Article 5*

### **Designated Authorities for the purpose of law enforcement access**

1. Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Regulation. 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.
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 6*

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

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.

---

<sup>1</sup> OJ 45, 14.6.1962, p. 1385.



## Article 7

### 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.

↓ 2725/2000/EC (adapted)

⇒ new

## Article 8

### Statistics

- ~~3.1.~~ The ~~Central Unit~~ Agency shall draw up statistics on ~~its~~ the work of the Central System every ~~quarter~~ ⇒ month ⇐, indicating ⇒ in particular ⇐ :
- (a) the number of data sets transmitted on persons referred to in Articles 9(1), ~~8(1) and 11(1)~~ 14(1) and 17(1) ;
  - (b) the number of hits for applicants for ~~asylum~~ ⇒ international protection ⇐ who have lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State;
  - (c) the number of hits for persons referred to in Article ~~8(1)~~ 14(1) who have subsequently lodged an application for ~~asylum~~ ⇒ international protection ⇐ ;
  - (d) the number of hits for persons referred to in Article ~~11(1)~~ 17(1) who had previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State;
  - (e) the number of fingerprint data which the Central ~~Unit~~ ⇒ System ⇐ had to ⇒ repeatedly ⇐ request a ~~second time~~ from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;

↓ new

- (f) the number of requests for marking and unmarking transmitted in accordance with Article 18(1) and (2).

(g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under points (b) and (d) of this Article.

---

↓ 2725/2000/EC  
⇒ new

2. At the end of each year, statistical data shall be established in the form of a compilation of the ⇒ monthly ⇐ quarterly statistics drawn up since the beginning of Eurodac's activities ⇒ for that year ⇐, including an indication of the number of persons for whom hits have been recorded under ⇒ points ⇐ (b), (c), and (d). ⇒ The statistics shall contain a breakdown of data for each Member State. ⇐
- ~~4.~~ Pursuant to the procedure laid down in Article 23(2), the Central Unit may be charged with carrying out certain other statistical tasks on the basis of the data processed at the Central Unit.
- 

↓ 2725/2000/EC (adapted)  
⇒ new

## CHAPTER II

# APPLICANTS FOR ~~ASYLUM~~ INTERNATIONAL PROTECTION

### *Article 9 4*

#### **Collection, transmission and comparison of fingerprints**

1. Each Member State shall promptly take the fingerprints of all fingers of every applicant for ~~asylum~~ ⇒ international protection ⇐ of at least 14 years of age and shall promptly ⇒ as soon as possible and no later than 72 hours after the lodging of that application for international protection as defined by Article 20(2) of the Dublin Regulation ⇐ transmit  them together with  the data referred to in points ~~(a)~~ (b) to ~~(f)~~ (g) of Article ~~5(1)~~ 11 to the Central Unit ⇒ System ⇐.
- 

↓ new

⇒ Non compliance with the 72 hours time limit does not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25 of this Regulation, the Member State of origin shall retake the

fingerprints of the applicant and resend them as soon as possible and no later than 48 hours after they have been successfully taken. ↩

↓ 2725/2000/EC

~~(2) The data referred to in Article 5(1) shall be immediately recorded in the central database by the Central Unit, or, provided that the technical conditions for such purposes are met, directly by the Member State of origin.~~

↓ new

2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.

↓ 2725/2000/EC (adapted)  
⇒ new

3. Fingerprint data within the meaning of point ~~(b)~~ (a) of Article ~~5(1) 11~~, transmitted by any Member State, ~~⊗~~ with exception to those transmitted in accordance with Article 10 point (b) ~~⊗~~ shall be compared ⇒ automatically ↩ with the fingerprint data transmitted by other Member States and already stored in the Central database ⇒ System ↩.
4. The Central Unit ⇒ System ↩ shall ensure, on the request of a Member State, that the comparison referred to in paragraph 3 covers the fingerprint data previously transmitted by that Member State, in addition to the data from other Member States.
5. The Central Unit ⇒ System ↩ shall ~~forthwith~~ ⇒ 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 Article ~~5(1) 8(a) to (g)~~ ~~⊗~~ although in the case of the data referred to in Article 5(1)(b), only insofar as they were the basis for the hit ⇒ along with, where appropriate, the mark referred to in Article 18(1) ↩.

~~Direct transmission to the Member State of origin of the result of the comparison shall be permissible where the technical conditions for such purpose are met.~~

- ~~7. The implementing rules setting out the procedures necessary for the application of paragraphs 1 to 6 shall be adopted in accordance with the procedure laid down in Article 22(1).~~

*Article 10***Information on the status of the data subject**

The following information shall be sent to the Central System in order to be stored in accordance with Article 9 for the purpose of transmission under Article 9(5):

- (a) When an applicant for international protection or another person as referred to in point (d) of Article 18(1) of the Dublin Regulation arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take him/her back as referred to in Article 24 of the Dublin Regulation, the responsible Member State shall update its dataset recorded in conformity with Article 8 of this Regulation relating to the person concerned by adding their date of arrival .
- (b) When an applicant for international protection arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take charge of them as referred to in Article 22 of the Dublin Regulation, the responsible Member State shall send a dataset in conformity with Article 11 of this Regulation relating to the person concerned and include their date of arrival.
- (c) As soon as the Member State of origin can establish that the person concerned whose data was recorded in EURODAC in accordance with Article 11 of this Regulation has left the territory of the Member States, it shall update its dataset recorded in conformity with Article 11 of this Regulation relating to the person concerned by adding the date when the person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of the Dublin Regulation.
- (d) As soon as the Member State of origin ensures that the person concerned whose data was recorded in EURODAC in accordance with Article 11 has left the territory of the Member States in compliance with a return decision or removal order it issued following the withdrawal or rejection of the application as provided for in Article 19(3) of the Dublin Regulation, it shall update its dataset recorded in conformity with Article 11 relating to the person concerned by adding the date of his/her removal or when the person left the territory.
- (e) The Member State which assumes responsibility in accordance with Article 17(1) of the Dublin Regulation shall update its dataset recorded in conformity with Article 11 of this Regulation relating to that applicant by adding the date when the decision to examine the application was taken.

---

↓ 2725/2000/EC  
⇒ new

Article 11 5  
**Recording of data**

1. Only the following data shall be recorded in the eCentral database ⇒ System ⇐ :

(~~ab~~) fingerprint data;

(~~ba~~) Member State of origin, place and date of the application for asylum ⇒ international protection; in the cases referred to in point (b) of Article 10, the date of application shall be the one entered by the Member State who transferred the applicant ⇐ ;

(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 Unit ⇒ System ⇐ ;

(~~g~~) ~~date on which the data were entered in the central database ;~~

---

↓ new

(g) operator user ID.

---

↓ 2725/2000/EC  
⇒ new

(~~h~~) ~~details in respect of the recipient(s) of the data transmitted and the date(s) of transmission(s).~~

(h) where applicable in accordance with Article 10 point (a) or point (b), the date of the arrival of the person concerned after a successful transfer;

(i) where applicable in accordance with Article 10 point (c), the date when the person concerned left the territory of the Member States;

(j) where applicable in accordance with Article 10 point (d), the date when the person concerned left or was removed from the territory of the Member States;

(k) where applicable in accordance with Article 10 point (e), the date when the decision to examine the application was taken.

~~2. After recording the data in the central database, the Central Unit shall destroy the media used for transmitting the data, unless the Member State of origin has requested their return.~~

*Article ~~12~~ 6*  
**Data storage**

Each set of data, as referred to in Article ~~5(1)~~ 11, shall be stored in the ~~Central database~~ ⇒ **System** ⇐

Upon expiry of this period, the Central ~~Unit~~ ⇒ **System** ⇐ shall automatically erase the data from the ~~Central database~~ ⇒ **System** ⇐.

*Article ~~13~~ 7*  
**Advance data erasure**

1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article ~~6~~ 12 shall be erased from the Central ~~Unit~~ ⇒ **System** ⇐, in accordance with Article ~~15(3)~~ 27(4) as soon as the Member State of origin becomes aware that the person has acquired such citizenship.

---

↓ new

- 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 9(1) or Article 14(1).

---

↓ 2725/2000/EC (adapted)  
⇒ new

### CHAPTER III

## ~~ALIENS~~ **THIRD COUNTRY NATIONALS OR STATELESS PERSONS** ~~APPREHENDED~~ **APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER**

*Article ~~14~~ 8*  
**Collection and transmission of fingerprint data**

- ~~1. Each Member State shall, in accordance with the safeguards laid down in the European Convention on Human Rights and in the United Nations Convention on the Rights of the~~

~~Child~~ promptly take the fingerprints of all fingers of every ~~alien~~  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  or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn them back  .

2. The Member State concerned shall promptly  as soon as possible and no later than 72 hours from the date of apprehension  transmit to the Central ~~Unit~~  System  the following data in relation to any ~~alien~~  third country national or stateless person , as referred to in paragraph 1, who is not turned back:

(a) fingerprint data;

(b) Member State of origin, place and date of the 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 ~~Unit~~  System  ;

---

(g) operator user ID.

3. By way of derogation from paragraph 2, as regards persons apprehended in the manner described in paragraph 1 who remain physically on the territory of the Member States but are kept in custody, confinement or detention upon their apprehension for a period exceeding 72 hours, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their release from custody, confinement or detention.
4. Non compliance with the 72 hours time limit referred to in paragraph 2 does not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.
5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person or the protection of public health, the Member State concerned shall take and send the fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.

*Article 15 9*  
**Recording of data**

1. The data referred to in ~~Article 5(1)(g) and in Article 8(2) 14(2)~~ shall be recorded in the ~~central database~~ ⇒ Central System ⇐.

Without prejudice to Article ~~3(3)8~~, data transmitted to the Central Unit ⇒ System ⇐ pursuant to Article ~~8(2) 14(2)~~ shall be recorded for the sole purpose of comparison with data on applicants for ~~asylum~~ ⇒ international protection ⇐ transmitted subsequently to the Central Unit ⇒ System ⇐.

The Central Unit ⇒ System ⇐ shall not compare data transmitted to it pursuant to Article ~~8(2) 14(2)~~ with any data previously recorded in the ~~central database~~ ⇒ Central System ⇐, nor with data subsequently transmitted to the Central Unit ⇒ System ⇐ pursuant to Article ~~8(2) 14(2)~~.

2. ~~The procedures provided for in Article 4(1), second sentence, Article 4(2) and Article 5(2) as well as the provisions laid down pursuant to Article 4(7) shall apply.~~ As regards the comparison of data on applicants for ~~asylum~~ ⇒ international protection ⇐ subsequently transmitted to the Central Unit ⇒ System ⇐ with the data referred to in paragraph 1, the procedures provided for in Article ~~4(3), (5) and (6) 9(3) and (5) and in Article 25(4)~~ shall apply.

*Article 16 10*  
**Storage of data**

1. Each set of data relating to an ~~alien~~ ☒ third country national or stateless person ☒ as referred to in Article ~~8(1) 14(1)~~ shall be stored in the ~~central database~~ ⇒ Central System ⇐ for ⇒ one year ⇐ ~~two years~~ from the date on which the fingerprints of the ~~alien~~ ☒ third country national or stateless person ☒ were taken. Upon expiry of this period, the Central Unit ⇒ System ⇐ shall automatically erase the data from the ~~central database~~ ⇒ Central System ⇐.
2. The data relating to an ~~alien~~ ☒ third country national or stateless person ☒ as referred to in Article ~~8(1) 14(1)~~ shall be erased from the ~~central database~~ ⇒ Central System ⇐ in accordance with Article ~~15(3) 28(3)~~ ☒ as soon as ☒ the Member State of origin becomes aware of one of the following circumstances before the ~~two~~ ⇒ one ⇐ -year period mentioned in paragraph 1 has expired:
  - (a) the ~~alien~~ ☒ third country national or stateless person ☒ has been issued with a residence ~~permit~~ ☒ document ☒ ;



(b) the ~~alien~~ ☒ third country national or stateless person ☒ has left the territory of the Member States;

(c) the ~~alien~~ ☒ third country national or stateless person ☒ has acquired the citizenship of any Member State.

↓ new

3. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).

4. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (c) of paragraph 2 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

↓ 2725/2000/EC (adapted)  
⇒ new

## CHAPTER IV

# ~~ALIENS~~ ☒ ~~THIRD COUNTRY NATIONALS OR STATELESS PERSONS~~ ☒ ~~FOUND ILLEGALLY PRESENT~~ ☒ ~~STAYING~~ ☒ ~~IN A MEMBER STATE~~

### *Article 17 ~~11~~*

#### **Comparison of fingerprint data**

1. With a view to checking whether an ~~alien~~ ☒ third country national or a stateless person ☒ found illegally ~~present~~ ☒ staying ☒ within its territory has previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State, each Member State may transmit to the Central ~~Unit~~ ⇒ System ⇐ any fingerprint data relating to fingerprints which it may have taken of any such ~~alien~~ ☒ 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 ~~alien~~ ☒ third country national or stateless person ☒ has previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State where:

- (a) the ~~alien~~  third country national or stateless person  declares that he/she has lodged an application for ~~asylum~~  ~~international protection~~  but without indicating the Member State in which he/she made the application;
- (b) the ~~alien~~  third country national or stateless person  does not request ~~asylum~~  ~~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 ~~alien~~  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 ~~Unit~~  ~~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 ~~aliens~~  third country nationals or stateless persons  referred to in paragraph 1.
3. The fingerprint data of an ~~alien~~  third country national or a stateless person  as referred to in paragraph 1 shall be transmitted to the Central ~~Unit~~  ~~System~~  solely for the purpose of comparison with the fingerprint data of applicants for ~~asylum~~  ~~international protection~~  transmitted by other Member States and already recorded in the ~~central database~~  ~~Central System~~ .

The fingerprint data of such an ~~alien~~  third country national or a stateless person  shall not be recorded in the ~~central database~~  ~~Central System~~ , nor shall they be compared with the data transmitted to the Central ~~Unit~~  ~~System~~  pursuant to Article ~~8(2)~~ 14(2).

4. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for ~~asylum~~  ~~international protection~~  transmitted by other Member States which have already been stored in the Central ~~Unit~~  ~~System~~ , the procedures provided for in Article ~~4(3) (5) and (6)~~ 9(3) and (5) as well as the provisions laid down pursuant to Article ~~4(7)~~ shall apply.
- ~~5. Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:~~

- ~~(a) erase the fingerprint data and other data transmitted to it under paragraph 1; and~~
- ~~(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.~~

## CHAPTER V

### ~~RECOGNISED REFUGEES~~ ~~⊗~~ PERSONS GRANTED INTERNATIONAL PROTECTION ~~⊗~~

#### *Article 12*

##### *Blocking of data*

~~1. Data relating to an applicant for asylum which have been recorded pursuant to Article 4(2) shall be blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member State of origin.~~

~~As long as a decision pursuant to paragraph 2 has not been adopted, hits concerning persons who have been recognised and admitted as refugees in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.~~

~~2. Five years after Eurodac starts operations, and on the basis of reliable statistics compiled by the Central Unit on persons who have lodged an application for asylum in a Member State after having been recognised and admitted as refugees in another Member State, a decision shall be taken in accordance with the relevant provisions of the Treaty, as to whether the data relating to persons who have been recognised and admitted as refugees in a Member State should:~~

~~(a) be stored in accordance with Article 6 for the purpose of the comparison provided for in Article 4(3); or~~

~~(b) be erased in advance once a person has been recognised and admitted as a refugee.~~

~~3. In the case referred to in paragraph 2(a), the data blocked pursuant to paragraph 1 shall be unblocked and the procedure referred to in paragraph 1 shall no longer apply.~~

~~4. In the case referred to in paragraph 2(b):~~

~~(a) data which have been blocked in accordance with paragraph 1 shall be erased immediately by the Central Unit; and~~

~~(b) data relating to persons who are subsequently recognised and admitted as refugees shall be erased in accordance with Article 15(3), as soon as the Member State of origin becomes aware that the person has been recognised and admitted as a refugee in a Member State.~~

~~5. The implementing rules concerning the procedure for the blocking of data referred to in paragraph 1 and the compilation of statistics referred to in paragraph 2 shall be adopted in accordance with the procedure laid down in Article 22(1).~~

*Article 18*  
**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 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5).
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 or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.

**CHAPTER VI**

**PROCEDURE FOR COMPARISON AND DATA TRANSMISSION  
FOR LAW ENFORCEMENT PURPOSES**

*Article 19*

**Procedure for comparison of fingerprint data with EURODAC data**

1. The designated authorities referred to in Article 5(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 20 or Article 21, 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 20 or Article 21 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 that have accessed it and they shall inform the verifying authority of such destruction.

#### *Article 20*

##### **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 Decision 2008/615/JHA 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;
  - (b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and
  - (c) there are reasonable grounds to consider that such comparison with EURODAC data will 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 21*

##### **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 22*

##### **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, in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.

↓ 2725/2000/EC (adapted)  
⇒ new

## CHAPTER ~~VI~~ VII

### DATA ~~PROCESSING USE~~, DATA PROTECTION AND LIABILITY

#### Article ~~23~~ 13

#### Responsibility for data *processing 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 ~~5(1)~~ 11, Article ~~8(2)~~ 14(2) and Article ~~11(2)~~ 17(2) are lawfully transmitted to the Central ~~Unit~~ ⇒ System ⇐;
  - (c) data are accurate and up-to-date when they are transmitted to the Central ~~Unit~~ ⇒ System ⇐;
  - (d) without prejudice to the responsibilities of the ~~Commission~~ ⇒ Agency ⇐, data in the ~~central database~~ ⇒ Central System ⇐ are lawfully recorded, stored, corrected and erased;
  - (e) the results of fingerprint data comparisons transmitted by the Central ~~Unit~~ ⇒ System ⇐ are lawfully ~~processed~~ *used*.
2. In accordance with Article ~~14~~ 34, the Member State of origin shall ensure the security of the data referred to in paragraph 1 before and during transmission to the Central ~~Unit~~ ⇒ System ⇐ as well as the security of the data it receives from the Central ~~Unit~~ ⇒ System ⇐.
3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article ~~4(6)~~ 25(4).
4. The ~~Commission~~ ⇒ Agency ⇐ shall ensure that the Central ~~Unit~~ ⇒ System ⇐ is operated in accordance with the provisions of this Regulation and its implementing rules. In particular, the ~~Commission~~ ⇒ Agency ⇐ shall:

- (a) adopt measures ensuring that persons working ~~in~~ with ~~in~~ the Central Unit ~~⇒~~ System ~~⇐~~ process use the data recorded ~~in~~ therein ~~in~~ the central database only in accordance with the purpose of ~~Eurodac~~EURODAC as laid down in Article 1(1);
- (b) ~~ensure that persons working in the Central System comply with all requests from Member States made pursuant to this Regulation in relation to recording, comparison, correction and erasure of data for which they are responsible;~~
- (b) ~~(c)~~ take the necessary measures to ensure the security of the Central Unit ~~⇒~~ System ~~⇐~~ in accordance with Article ~~14~~ 34;
- (c) ~~(d)~~ ensure that only persons authorised to work ~~in~~ with ~~in~~ the Central Unit ~~⇒~~ System ~~⇐~~ have access ~~to~~ thereto ~~to~~ data recorded in the central database, without prejudice to Article 20 and the powers of the independent supervisory body which will be established under Article 286(2) of the Treaty ~~and~~ the competences of the European Data Protection Supervisor ~~and~~.

The Commission ~~⇒~~ Agency ~~⇐~~ shall inform the European Parliament and the Council ~~⇒~~ as well as the European Data Protection Supervisor ~~⇐~~ of the measures it takes pursuant to the first subparagraph.

↓ 407/2002/EC Article 2 (adapted)  
⇒ new

#### Article 24 ~~2~~ Transmission

1. Fingerprints shall be digitally processed and transmitted in the data format referred to in Annex I. As far as it is necessary for the efficient operation of the Central Unit ~~⇒~~ System ~~⇐~~, the Central Unit ~~⇒~~ Agency ~~⇐~~ shall establish the technical requirements for transmission of the data format by Member States to the Central Unit ~~⇒~~ System ~~⇐~~ and vice versa. The Central Unit ~~⇒~~ Agency ~~⇐~~ shall ensure that the fingerprint data transmitted by the Member States can be compared by the computerised fingerprint recognition system.
2. Member States ~~should~~ shall ~~transmit~~ transmit the data referred to in Article ~~5(1)~~ 11(1), Article 14(2) and Article 17(2) of the Eurodac Regulation electronically. ~~⇒~~ The data referred to in Article 11(1) and Article 14(2) shall be automatically recorded in the Central System. ~~⇐~~ As far as it is necessary for the efficient operation of the Central Unit ~~⇒~~ System ~~⇐~~, the Central Unit ~~⇒~~ Agency ~~⇐~~ shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central Unit ~~⇒~~ System ~~⇐~~ and vice versa. ~~Transmission of data in paper form using the form set out in Annex II or by other means of data support (diskettes, CD-ROM or other means of data support which may be developed and generally used in future) should be limited to situations in which there are continuous technical problems.~~

3. The reference number referred to in Article ~~5(1)(d)~~ 11(d) and Article 14(2)(d) and 17(1) ~~of the Eurodac Regulation~~ shall make it possible to relate data unambiguously to one particular person and to the Member State which is transmitting the data. In addition, it shall make it possible to tell whether such data relate to ~~an asylum-seeker or a person referred to in Article 8 or Article 11 of the Eurodac Regulation~~9, Article 14 or Article 17.
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 ~~asylum-seekers~~  persons referred to in Article 9(1) , "2" to persons referred to in Article ~~8~~ 14(1) ~~of the Eurodac Regulation~~ and "3" to persons referred to in Article ~~11~~ 17 ~~of the Eurodac Regulation~~.
5. The ~~Central Unit~~  Agency  shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central Unit  System .
64. The Central Unit  System  shall confirm receipt of the transmitted data as soon as possible. To this end the ~~Central Unit~~  Agency  shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.

#### *Article 25 3*

#### **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 it is necessary to ensure that the results of the comparison by the Central Unit  System  reach a very high level of accuracy, the ~~Central Unit~~  Agency  shall define the appropriate quality of transmitted fingerprint data. The Central Unit  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 Unit  System  shall, ~~as soon as possible,~~  inform  the Member State.  The Member State concerned shall  transmit fingerprint data of the appropriate quality  using the same reference number of the previous set of fingerprint data .
2. The Central Unit  System  shall carry out comparisons in the order of arrival of requests. Each request must be dealt with within 24 hours. ~~In the case of data which are transmitted electronically, a~~ A Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where these times cannot be respected owing to circumstances which are outside the ~~Central Unit~~  Agency's  responsibility, the Central Unit  System  shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as it is necessary for the efficient operation of the Central Unit  System , the ~~Central Unit~~  Agency  shall establish criteria to ensure the priority handling of requests.
3. As far as it is necessary for the efficient operation of the Central Unit  System , the ~~Central Unit~~  Agency  shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.



↓ 2725/2000/EC Article 4(6) (adapted)  
⇒ new

4. The results of the comparison shall be immediately checked in the Member State of origin ⇒ by a fingerprint expert ⇐. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to Article ~~15~~ 32 of the Dublin ~~Convention~~ ⊗ Regulation ⊗.

Information received from the Central ~~Unit~~ ⇐ System ⇐ relating to other data found to be unreliable shall be erased ~~or destroyed~~ as soon as the unreliability of the data is established.

↓ new

5. Where final identification in accordance with paragraph 4 reveal that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the Commission and to the Agency.

↓ 407/2002/EC (adapted)  
⇒ new

#### *Article ~~26~~ 4*

#### **Communication between Member States and the Central ~~Unit~~ ⇐ System ⇐**

Data transmitted from the Member States to the Central ~~Unit~~ ⇐ System ⇐ and vice versa shall use ~~IDA generic services referred to in Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA)~~ ⇐ the EURODAC Communication Infrastructure ⇐. As far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇐ System ⇐, the ~~Central Unit~~ ⊗ Agency ⊗ shall establish the technical procedures necessary for the use of ~~IDA generic services~~ ⇐ the Communication ⇐.

#### *Article ~~14~~* **Security**

1. ~~The Member State of origin shall take the necessary measures to:~~
- (a) ~~prevent any unauthorised person from having access to national installations in which the Member State carries out operations in accordance with the aim of Eurodac (checks at the entrance to the installation);~~
  - (b) ~~prevent data and data media in Eurodac from being read, copied, modified or erased by unauthorised persons (control of data media);~~

- ~~(c) guarantee that it is possible to check and establish a posteriori what data have been recorded in Eurodac when and by whom (control of data recording);~~
- ~~(d) prevent the unauthorised recording of data in Eurodac and any unauthorised modification or erasure of data recorded in Eurodac (control of data entry);~~
- ~~(e) guarantee that, in using Eurodac, authorised persons have access only to data which are within their competence (control of access);~~
- ~~(f) guarantee that it is possible to check and establish to which authorities data recorded in Eurodac may be transmitted by data transmission equipment (control of transmission);~~
- ~~(g) prevent the unauthorised reading, copying, modification or erasure of data during both the direct transmission of data to or from the central database and the transport of data media to or from the Central Unit (control of transport);~~

2. ~~As regards the operation of the Central Unit, the Commission shall be responsible for applying the measures mentioned under paragraph 1.~~

↓ 2725/2000/EC  
⇒ new

#### Article ~~27~~ 15

#### Access to, and correction or erasure of, data recorded in ~~Eurodac~~EURODAC

1. The Member State of origin shall have access to data which it has transmitted and which are recorded in the ~~central database~~ ⇒ 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 ~~4(5)~~ 9(5).

↓ 2725/2000/EC (adapted)  
⇒ new

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the ~~central database~~ ⇒ Central System ⇐ shall be those designated by each Member State ⇒ for the purpose of Article 1(1). This designation shall specify the exact 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 Agency ⇐ a list of those authorities ⇒ and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency 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 Unit  $\Rightarrow$  System  $\Leftarrow$  by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article ~~6, Article 10(1) or Article 12(4)(a)~~ 12 or Article 16(1).

~~Where the Member State of origin records data directly in the central database, it may amend or erase the data directly.~~

~~Where the Member State of origin does not record data directly in the central database, the Central Unit shall amend or erase the data at the request of that Member State.~~

4. If a Member State or the Central Unit  $\Rightarrow$  Agency  $\Leftarrow$  has evidence to suggest that data recorded in the ~~central database~~  $\Rightarrow$  Central System  $\Leftarrow$  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 database~~  $\Rightarrow$  Central System  $\Leftarrow$  contrary to this Regulation, it shall ~~similarly~~ advise  $\Rightarrow$  the Agency, the Commission and  $\Leftarrow$  the Member State of origin as soon as possible. The latter shall check the data concerned and, if necessary, amend or erase them without delay.

5. The Central Unit  $\Rightarrow$  Agency  $\Leftarrow$  shall not transfer or make available to the authorities of any third country data recorded in the ~~central database~~  $\Rightarrow$  Central System  $\Leftarrow$ , unless it is specifically authorised to do so in the framework of a Community agreement on the criteria and mechanisms for determining the State responsible for examining an application for ~~asylum~~  $\Rightarrow$  international protection  $\Leftarrow$  .

## ~~Article 22~~

### *Implementing rules*

- ~~1. The Council shall adopt, acting by the majority laid down in Article 205(2) of the Treaty, the implementing provisions necessary for~~

~~– laying down the procedure referred to in Article 4(7);~~

~~– laying down the procedure for the blocking of the data referred to in Article 12(1);~~

~~– drawing up the statistics referred to in Article 12(2).~~

~~In cases where these implementing provisions have implications for the operational expenses to be borne by the Member States, the Council shall act unanimously.~~

- ~~2. The measures referred to in Article 3(4) shall be adopted in accordance with the procedure referred to in Article 23(2).~~

*Article 28 16*

**Keeping of records ~~by the Central Unit~~**

1. The ~~Central Unit~~ ⇒ **Agency** ⇐ shall keep records of all data processing operations within the ~~Central Unit~~ ⇒ **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 ~~putting~~ ⇐ entering ⇐ in 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 ~~14~~ 34. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year ⇒ **after the retention period referred to in Article 12 and in Article 16(1) has expired** ⇐, if they are not required for monitoring procedures which have already begun.

---

↓ new

3. **Each Member State shall take the necessary measures in order to achieve the objectives set out in paragraph 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.**

---

↓ 2725/2000/EC (adapted)  
⇒ new

*~~Article 23~~*

*~~Committee~~*

- ~~1. The Commission shall be assisted by a committee.~~
- ~~2. In the cases where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply.~~

~~The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.~~
- ~~3. The committee shall adopt its rules of procedure.~~

*Article 29 18*

**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 or 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) ~~regarding~~ the purpose for which ~~the~~ his or her data will be processed within ~~Eurodac~~EURODAC  $\Rightarrow$  including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation  $\Leftarrow$ .
- (c) the recipients of the data;
- (d) in relation to a person covered by Article ~~4~~ 9 or Article ~~8~~ 14, the obligation to have his/her fingerprints taken;
- (e) the existence of the right of access to, ~~and the right to rectify,~~ the data ~~relating to~~ him/her ~~concerning him/her~~, and the right to request that inaccurate data relating to him/her be corrected  $\Leftarrow$   $\Rightarrow$  or that unlawfully processed data relating to them be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 31(1)  $\Leftarrow$ .

In relation to a person covered by Article ~~4~~ 9 or Article ~~8~~ 14, 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 ~~11~~ 17, the information referred to in the first subparagraph shall be provided no later than the time when the data relating to the person are transmitted to the Central ~~Unit~~  $\Rightarrow$  System  $\Leftarrow$ . This obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.

$\Downarrow$  new

A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 4(1) of the Dublin Regulation shall be drawn up in accordance with the procedure referred to in Article 40(2) of the Dublin Regulation. The leaflet should be "clear and simple, drafted in a language that the person understands or may reasonably be presumed to understand.

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

$\Downarrow$  2725/2000/EC  
 $\Rightarrow$  new

2. In each Member State any data subject may, in accordance with the laws, regulations and procedures of that 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 database~~  $\Rightarrow$  Central System  $\Leftarrow$  and of the Member State which transmitted them to the Central ~~Unit~~  $\Rightarrow$  System  $\Leftarrow$ . 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 Member State, or States, in question so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the ~~central database~~ ⇒ Central System ⇐.
5. If it emerges that data recorded in the ~~central database~~ ⇒ 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 ~~15(3)~~ 27(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 database~~ ⇒ 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.

---

 new

9. Whenever a person requests data relating to him or 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 this document available to the National Supervisory Authorities without delay, upon their request.

- ~~9.~~ 10. In each Member State, the national supervisory authority shall ⇒ on the basis of his/her request, ⇐ assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his/her rights.
- ~~10.~~ 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. ~~The data subject may also apply for assistance and advice to the joint supervisory authority set up by Article 20.~~
- ~~11.~~ 12. In each Member State any person may, in accordance with the laws, regulations and procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he/she is refused the right of access provided for in paragraph 2.
- ~~12.~~ 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 State concerning the data relating to him/her recorded in the ~~central database~~ ⇒ 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 ~~10~~ 13, shall subsist throughout the proceedings.

Article ~~30~~ 19

~~⊗~~ Supervision by the ~~⊗~~ National ~~S~~upervisory ~~A~~uthority

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 respective 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 ~~Unit~~ ⇒ System ⇐.
2. Each Member State shall ensure that its national supervisory authority has access to advice from persons with sufficient knowledge of fingerprint data.

*Article 31***Supervision by the European Data Protection Supervisor**

1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.
2. The European Data Protection Supervisor shall ensure that an audit of the Agency'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 Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.

*Article 32***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 Agency every two years.

*Article 33***Protection of personal data for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences**

1. The Framework Decision 2008/977/JHA is applicable to the processing of relevant personal data for law enforcement purposes under this Regulation.
2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA.



3. Personal data obtained pursuant to this Regulation 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 Regulation 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 Regulation 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 34*

#### **Data security**

1. The Member State of origin shall ensure the security of the data before and during transmission to 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 erasure of stored personal data (storage control);
  - (e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or erasure 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, erase and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 25 of 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 erasure 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. The Agency 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.

#### *Article 35*

#### **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 Regulation 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.

#### *Article 36*

#### **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 Regulation 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 19(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 38. 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.

↓ 2725/2000/EC  
⇒ new

*Article ~~37~~ 17*  
**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 laid down in this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That 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 failure of a Member State to comply with its obligations under this Regulation causes damage to the ~~central database~~ ⇒ **Central System** ⇐, that Member State shall be held liable for such damage, unless and insofar as the ~~Commission~~ ⇒ **Agency 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.

## CHAPTER VIII

### AMENDMENTS TO THE REGULATION (EU) No 1077/2011

#### Article 38

#### Provisions amending Regulation (EU) No 1077/2011

1. Article 5 is replaced by the following:

#### “Article 5

#### Tasks relating to EURODAC

In relation to EURODAC, the Agency shall perform :

(a) the tasks conferred on the Agency by Regulation (EU) No .../.... *[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...}]*.

(b) tasks relating to training on the technical use of EURODAC.”

2. Article 12(1) is amended as follows:

- (a) points (t), (u) and (v) are replaced by the following:

“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No .../... *[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) 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 to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes;

(u) to adopt the annual report on the activities of the Central System of EURODAC pursuant to Article 40(1) of Regulation (EU) No .../.... *[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...]*;

(v) to make comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45 of Regulation (EC) 1987/2006 , Article 42(2) of Regulation (EC) No 767/2008 and Article 31 (2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../....] and ensure appropriate follow-up of the audit;”

(b) point (x) is replaced by the following:

“(x) to compile statistics on the work of the Central System of EURODAC pursuant to Article 8(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../....}]”

(c) point (z) is replaced by the following:

“(z) to ensure annual publication of the list of authorities designated pursuant to Article 27(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../....]”

3. In Article 15 paragraph (4) is replaced by the following:

“4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, is on the agenda or when a question concerning EURODAC, in relation with the application of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../....] is on the agenda.”

4. Article 17 is amended as follows:

(a) in paragraph 5 point (g) is replaced by the following:

“(g) without prejudice to Article 17 of the Staff Regulations, establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA and Article 26(9) of Regulation (EC) No 767/2008 respectively and Article 4(6) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../....];”

(b) in paragraph 6 point (i) is replaced by the following:

“(i) reports on the technical functioning of each large-scale IT system referred to in point (t) of Article 12(1) and the annual report on the activities of the Central System of EURODAC referred to in point (u) of Article 12(1), on the basis of the results of monitoring and evaluation.”

5. In Article 19 paragraph 3 is replaced by the following:

"3. Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and to the EURODAC Advisory Groups."

↓ 2725/2000/EC (adapted)  
⇒ new

## CHAPTER ~~VII~~ IX

### FINAL PROVISIONS

#### Article ~~39~~ 21 Costs

1. The costs incurred in connection with the establishment and operation of the ~~Central Unit~~ ⇒ **Central System and the Communication Infrastructure** ⇐ shall be borne by the general budget of the European Union.
2. The costs incurred by national ⇒ **access points** ⇐ ~~units~~ and the costs for connection to the ~~central database~~ ⇒ **Central System** ⇐ shall be borne by each Member State.
3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of the criminal offences defined in this Regulation.
- ~~3. The costs of transmission of data from the Member State of origin and of the findings of the comparison to that State shall be borne by the State in question.~~

#### Article ~~40~~ 24 Annual report; ~~m~~ **Monitoring and evaluation**

1. The ~~Commission~~ ⇒ **Agency** ⇐ shall submit to the European Parliament and the Council an annual report on the activities of the Central ~~Unit~~ ⇒ **System** ⇐. The annual report shall include information on the management and performance of ~~Eurodac~~ **EURODAC** against pre-defined quantitative indicators for the objectives referred to in paragraph 2.
2. The ~~Commission~~ ⇒ **Agency** ⇐ shall ensure that ☒ procedures ☒ ~~systems~~ are in place to monitor the functioning of the Central ~~Unit~~ ⇒ **System** ⇐ against objectives ☒ relating to ☒ ~~in terms of~~ outputs, cost-effectiveness and quality of service.

3. ~~The Commission shall regularly evaluate the operation of the Central Unit in order to establish whether its objectives have been attained cost-effectively and with a view to providing guidelines for improving the efficiency of future operations.~~
  4. ~~One year after Eurodac starts operations, the Commission shall produce an evaluation report on the Central Unit, focusing on the level of demand compared with expectation and on operational and management issues in the light of experience, with a view to identifying possible short-term improvements to operational practice.~~
- 

↓ new

3. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in the Central System.
  4. Every two years, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.
- 

↓ 2725/2000/EC  
⇒ new

5. ~~Three years after Eurodac starts operations~~ ⇒ the start of application of this Regulation as provided for in Article 46(2) ⇐ and every ~~six~~ ⇒ four ⇐ years thereafter, the Commission shall produce an overall evaluation of ~~Eurodac~~EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations ⇒ , as well as make any necessary recommendations ⇐ . ⇒ The Commission shall transmit the evaluation to the European Parliament and the Council. ⇐
- 

↓ new

6. Member States shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraph 4 and 5.
7. The Agency shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.
8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, 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.

9. The Agency, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.

↓ 2725/2000/EC (adapted)  
⇒ new

#### *Article 41 ~~25~~* **Penalties**

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

#### *Article 42 ~~26~~* **Territorial scope**

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

↓ new

#### *Article 43* **Notification of designated authorities and verifying authorities**

1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission 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 Regulation] at the latest each Member State shall notify the Commission 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 Regulation] at the latest Europol shall notify the Commission 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.
- 

↓ new

#### Article 44

#### **Transitional provision**

Data blocked in the Central System in accordance with Article 12 of Council Regulation (EC) No 2725/2000/EC shall be unblocked and marked in accordance with Article 18(1) of this Regulation on the date provided for in Article 46 of this Regulation.

#### Article 45

#### **Repeal**

Council Regulation (EC) No 2725/2000 of 11 December 2000 and Council Regulation (EC) No 407/2002 are repealed with effect from the date referred to in Article 46(2).

References to the repealed Regulations shall be read in accordance with the correlation table in Annex III.

---

↓ 2725/2000/EC Article 27 (adapted)  
⇒ new

#### Article ~~46~~ 27

#### **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 ~~Communities~~ ~~⊗~~ Union ~~⊗~~.
2. This Regulation shall apply ⇒ two years from the date of the entry into force of this Regulation. ⇐ , and Eurodac shall start operations, from the date which the Commission shall publish in the Official Journal of the European Communities, when the following conditions met:
  - (a) ~~each Member State has notified the Commission that it has made the necessary technical arrangements to transmit data to the Central Unit in accordance with the implementing rules adopted under Article 4(7) and to comply with the implementing rules adopted under Article 12(5); and~~
  - (b) ~~the Commission has made the necessary technical arrangements for the Central Unit to begin operations in accordance with the implementing rules adopted under Article 4(7) and Article 12(5).~~

---

↓ new

3. Member States shall notify the Commission and the Agency as soon as they have made the technical arrangements to transmit data to the Central System, and in any event no later than two years from the date of the entry into force of this Regulation.
4. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

---

↓ 2725/2000/EC

Done at Brussels,

*For the European Parliament*  
*The President*

*For the Council*  
*The President*

---

↓ 407/2002/EC ⇒ new
------------------------

### Annex I

#### **Data format for the exchange of fingerprint data**

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

~~ANSI/NIST-CSL-1-1993~~ ⇒ 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

## EURODAC – Fingerprint form

1.	Reference number			
2.	Place of the application for asylum or place where the third country national or stateless person was apprehended			
3.	Date of the application for asylum or date on which the third country national or stateless person was apprehended			
4.	Sex			
5.	Date on which the fingerprints were taken			
6.	Date on which the data were transmitted to the Central System			

105 mm from top of form

155 mm from top of form

205 mm from top of form

### ROLLED IMPRESSIONS

1. Right thumb	2. Right forefinger	3. Right middle finger	4. Right ring finger	5. Right little finger
50 mm	40 mm	40 mm	40 mm	40 mm
40 mm				40 mm
6. Left thumb	7. Left forefinger	8. Left middle finger	9. Left ring finger	10. Left little finger
40 mm				

### PLAIN IMPRESSIONS

LEFT HAND Four fingers taken simultaneously 75 mm 65 mm	TWO THUMBS Impressions taken simultaneously		RIGHT HAND Four fingers taken simultaneously 75 mm
	LEFT	RIGHT	
	30 mm	30 mm	



**ANNEX II**  
**Repealed Regulations**  
**(referred to in Article 45)**

Council Regulation (EC) No 2725/2000/EC (OJ L 316, 15.12.2000, p. 1.)

Council Regulation (EC) No 407/2002/EC (OJ L 062, 05.03.2002 p. 1.)

**ANNEX III**  
**Correlation table**

<b>Regulation 2725/2000/EC</b>	<b>This Regulation</b>
Article 1(1)	Article 1(1)
Article 1(2), first subparagraph	Article 3(1)
Article 1(2), second subparagraph	Deleted
Article 1(2), third subparagraph	Article 3(4)
Article 1(3)	Article 1(3)
Article 2	Article 2
Article 3(1)	deleted
Article 3(2)	Article 3(3)
Article 3(3)	Article 8
Article 3(4)	Deleted
Article 4(1)	Article 9(1), 3(5)
Article 4(2)	Deleted
Article 4(3)	Article 9(3)
Article 4(4)	Article 9(4)
Article 4(5)	Article 9(5)
Article 4(6)	Article 25(4)
Article 5	Article 11
Article 6	Article 12
Article 7	Article 13
Article 8	Article 14
Article 9	Article 15

Article 10	Article 16
Article 11(1)-(4)	Article 17(1)-(4)
Article 11(5)	Deleted
Article 12	Article 18
Article 13	Article 23
Article 14	Deleted
Article 15	Article 27
Article 16	Article 28
Article 17	Article 37
Article 18	Article 29
Article 19	Article 30
Article 20	Deleted
Article 21	Article 39
Article 22	Deleted
Article 23	Deleted
Article 24	Article 40
Article 25	Article 24
Article 26	Article 42
Article 27	Article 46

<b>Regulation 407/2002/EC</b>	<b>This Regulation</b>
Article 2	Article 24
Article 3	Article 25
Article 4	Article 26
Article 5(1)	Article 3(3)
Annex I	Annex I
Annex II	Deleted



## LEGISLATIVE FINANCIAL STATEMENT

### **1. FRAMEWORK OF THE PROPOSAL/INITIATIVE**

- 1.1. Title of the proposal/initiative
- 1.2. Policy area(s) concerned in the ABM/ABB structure
- 1.3. Nature of the proposal/initiative
- 1.4. Objective(s)
- 1.5. Grounds for the proposal/initiative
- 1.6. Duration and financial impact
- 1.7. Management method(s) envisaged

### **2. MANAGEMENT MEASURES**

- 2.1. Monitoring and reporting rules
- 2.2. Management and control system
- 2.3. Measures to prevent fraud and irregularities

### **3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE**

- 3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected
- 3.2. Estimated impact on expenditure
  - 3.2.1. *Summary of estimated impact on expenditure*
  - 3.2.2. *Estimated impact on [body]'s appropriations*
  - 3.2.3. *Estimated impact on [body]'s human resources*
  - 3.2.4. *Compatibility with the current multiannual financial framework*
  - 3.2.5. *Third-party participation in financing*
- 3.3. Estimated impact on revenue

## LEGISLATIVE FINANCIAL STATEMENT

### 11. FRAMEWORK OF THE PROPOSAL/INITIATIVE

#### 11.1. Title of the proposal/initiative

Amended proposal for a Regulation of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) 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 to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

#### 11.2. Policy area(s) concerned in the ABM/ABB structure<sup>1</sup>

Area of Home Affairs (title 18)

Activity: Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (chapter 18.02.11)

#### 11.3. Nature of the proposal/initiative

- The proposal/initiative relates to **a new action**
- The proposal/initiative relates to **a new action following a pilot project/preparatory action**<sup>2</sup>
- The proposal/initiative relates to **the extension of an existing action**
- The proposal/initiative relates to **an action redirected towards a new action**

#### 11.4. Objectives

##### 11.4.1. *The Commission's multiannual strategic objective(s) targeted by the proposal/initiative*

Not applicable

##### 11.4.2. *Specific objective(s) and ABM/ABB activity(ies) concerned*

###### Specific objective No. 1

Contribute to the completion of the Common European Asylum System by adopting higher common standards of protection, supporting practical cooperation and increasing solidarity within the EU and between the EU and third countries with the support of the European Refugee Fund.

<sup>1</sup> ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

<sup>2</sup> As referred to in Article 49(6)(a) or (b) of the Financial Regulation.

Specific objective No. 2

Facilitate the prevention, detection and investigation of terrorist offences and other serious criminal offences.

ABM/ABB activity(ies) concerned

18 02 – Solidarity – External Borders, Return, Visa Policy and Free Movement of People

#### 11.4.3. *Expected result(s) and impact*

*Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.*

This proposal retains from the previous proposal [COM (2010) 555 final] the improvements of the system as regards new, asylum-focused functionalities and, at the same time, adds the functionality of law enforcement searches originally proposed in COM (2009) 342 final and COM (2009) 344 final.

The proposal will better manage and protect the data of data subjects while it will also facilitate Member States' procedures to determine the Member State responsible for the assessment of an asylum claim. It will facilitate prevention, detection and investigation of terrorist offences and other serious criminal offences by allowing access to EURODAC for consultation for law enforcement purposes.

#### 11.4.4. *Indicators of results and impact*

*Specify the indicators for monitoring implementation of the proposal/initiative.*

Concerning the improvements to the efficiency of EURODAC and the better addressing of data protection concerns, the indicators would be the annual statistics on the operation of EURODAC, eg. those on missed hits and wrong hits, transmission delays, etc., together with the four-yearly evaluation of EURODAC. The modification to "mark" data instead of "block" data as in the original Regulation should be implemented by the IT Agency within two years after the publication of this Regulation. Success will be measured through the annual EURODAC report that will highlight how many cases were marked, together with responses in the four-yearly evaluation from Member States noting whether this information permitted a transfer back to the country that should have been hosting the data subject. The change in the rules on deletion of data is designed to ensure that no EU citizen's data are stored in EURODAC. This can be tested when future nations accede to the EU (such as Croatia) to ensure that all data concerning Croatian nationals are deleted automatically. The success of this change will be reported in the four-yearly evaluation.

Concerning the facilitation of the prevention, detection and investigation of terrorist offences and other serious criminal offences, the indicators would be the statistics on the number of terrorist offences and other serious criminal offences prevented, detected and investigated as a result of a EURODAC consultation for law enforcement purposes. The IT modifications to permit comparisons with latent fingerprints should be completed by the IT Agency two years after the publication of this Regulation. It is not possible to anticipate the number of requests that will be made for law enforcement purposes, but if even only a few serious crimes are solved or prevented over a period of several years, the investment will have been merited. There are significant safeguards in the proposal designed to prevent excessive use of the law enforcement access tool (must be a serious crime as laid down by the European Arrest Warrant, and there must have been a Prüm check first) therefore one indicator of success will also be that the requests are limited only to those falling within these strict boundaries.

Statistics sets are requested in Article 40 of the Recast.

## 11.5. Grounds for the proposal/initiative

### 11.5.1. Requirement(s) to be met in the short or long term

As elaborated in the Explanatory Memorandum to the proposal in sections 1, 3, 5 and 7:

In order to inform Member States of the status of those applicants who have in fact been already granted international protection in a Member State, *data on refugees should be deblocked* (i.e. made available for searches).

In order to better facilitate the application of the Dublin Regulation, Member States will be required to *indicate in EURODAC the fact that they apply the sovereignty or the humanitarian clauses* provided for by that Regulation, ie. assume responsibility for the assessment of the claim of an applicant for whom they would not normally be responsible under the criteria of the Dublin Regulation.

In order to ensure *consistency with the asylum acquis*, the scope of the Regulation is proposed to be extended to cover subsidiary protection.

In order to ensure *consistency with the asylum acquis*, the storage period for data on third country nationals or stateless persons fingerprinted in connection with the irregular crossing of an external border is proposed to be aligned with the period until which Article 10(1) of the Dublin Regulation allocates responsibility on the basis of that information (i.e. one year).

Based on the outcome of negotiations in the Council, a new Article was introduced in order to provide information to Member States on the status of the data subject (asylum seekers or irregular entrant). This article foresees that Member States are also informed if a given person, whose data is stored in the database, was transferred following a Dublin take charge procedure, or if he or she left the territory of the Member States, either voluntarily or as the result of a return decision or removal order.

In order to facilitate prevention, detection and investigation of terrorist offences and other serious criminal offences, access for consultation for law enforcement purposes to EURODAC will be allowed.

### 11.5.2. Added value of EU involvement

Cross-border crime is increasing and presents one of the most serious threats to our society as reported by Europol. Without adequate and efficient cooperation between law enforcement authorities of Member States, including access to relevant information held in other Member States, it will be very difficult, if not impossible, for these authorities to perform their duties in relation to the prevention, detection and investigation of terrorists offences and other serious criminal offences and hence to fight such cross-border crime effectively. Because of the very nature of these crimes, instruments on an EU level are required to set the ground for cooperation between Member States.

In addition, action at the EU level will help to ensure harmonised provisions on safeguarding data protection, whereas if Member States are left to legislate independently, a harmonised level of safeguards will be difficult to achieve. Furthermore, absence of action at EU level would be detrimental for data protection as it compels law enforcement authorities to process

much more data than is required if they had access to a central index of available data. In addition, as the safeguards would not be harmonised at EU level, the level of protection of individuals with regard to the protection of their personal data could vary sensibly between Member States. The reason for this is that they have to resort to requests for the data to all Member States, rather than a single request to the relevant Member State. All these requests ultimately lead to the processing of much more data, which itself is detrimental to data protection.

As EURODAC is a fingerprint database run currently by the European Commission and in future by the IT Agency, it is only possible for the Union to make the necessary upgrades to the EURODAC system as identified by the last evaluation of EURODAC. The Central Unit needs to make the changes concerning the marking of data (instead of marking, as before). Member States wishing to access EURODAC for law enforcement purposes can only do so via a centrally coordinated system as provided for in this EURODAC Recast Regulation. The Union must therefore provide the basis through which the comparison of latent fingerprints from a crime scene may be made with live fingerprints taken in the course of applying for asylum. Such a comparison of data would not be possible without action at the level of the Union.

#### 11.5.3. *Lessons learned from similar experiences in the past*

EURODAC has been a successful operation database since 15 January 2003 containing the fingerprints of all asylum seekers within the EU. Most of its original specifications have served their intended functions well, but as shown by the evaluation of Dublin and EURODAC in 2007<sup>1</sup> it is necessary to make certain modifications to improve its usage. The majority of amendments made via this Recast Regulation are therefore on the basis of the lessons learned through the prior evaluation. In addition, using EURODAC for law enforcement purposes is a further efficiency as it will better utilise already existing data for only a small outlay of EU investment.

#### 11.5.4. *Coherence and possible synergy with other relevant instruments*

The present proposal was drafted in full coherence with the recast proposal on the Dublin Regulation.<sup>2</sup>

---

<sup>1</sup> COM(2007) 299 final

<sup>2</sup> Proposal for a Regulation of the European Parliament and of the Council 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, COM(2008) 820.

## 11.6. Duration and financial impact

- Proposal/initiative of **limited duration**
  - Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY
  - Financial impact from YYYY to YYYY
- Proposal/initiative of **unlimited duration**
  - Implementation with a start-up period from YYYY to YYYY,
  - followed by full-scale operation.

## 11.7. Management mode(s) envisaged<sup>1</sup>

- Centralised indirect management** with the delegation of implementation tasks to:
  - executive agencies
  - bodies set up by the European Union<sup>2</sup>
  - national public-sector bodies/bodies with public-service mission
  - persons entrusted with the implementation of specific actions pursuant to Title V of the Treaty on European Union and identified in the relevant basic act within the meaning of Article 49 of the Financial Regulation
- Joint management** with international organisations (*to be specified*)

*If more than one management mode is indicated, please provide details in the "Comments" section.*

### Comments

EURODAC will be transferred to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (the "IT Agency"). The additional features specified in the EURODAC Recast will be developed by the IT Agency.

<sup>1</sup> Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html)

<sup>2</sup> As referred to in Article 185 of the Financial Regulation.

## 12. MANAGEMENT MEASURES

### 12.1. Monitoring and reporting rules

*Specify frequency and conditions.*

Monitoring of the efficiency of the changes introduced by the present proposal is to be performed in the framework of the annual reports on the activities of the EURODAC Central Unit. Monitoring of data protection issues will be performed by the European Data Protection Supervisor.

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.

The original EURODAC Regulation contained Article 24 concerning evaluation of EURODAC. This Recast proposal also includes an Article (40) concerning monitoring and evaluation.

### 12.2. Management and control system

#### 12.2.1. Risk(s) identified

Failing to make important amendments to the Regulation in force, the efficiency of EURODAC could be undermined, as well as its supporting role to the implementation of the Dublin Regulation. Not being able to keep up with the changes of the asylum and data protection *acquis* would be also an important risk.

#### 12.2.2. Control method(s) envisaged

The indicators will be the statistics on the operation of EURODAC, eg. those on missed hits and wrong hits, transmission delays, etc.

### 12.3. Measures to prevent fraud and irregularities

*Specify existing or envisaged prevention and protection measures.*

In order to combat fraud, corruption and other unlawful activities, the provisions of Regulation (EC) No 1037/1999 shall apply without restriction to the Agency responsible for the operational management of EURODAC.

The Agency shall also accede to the interinstitutional Agreement concerning internal investigations by the European Antifraud Office (OLAF) and shall issue, without delay, the appropriate provisions applicable to all the employees of the Agency.

The decisions concerning funding and the implementation agreements and instruments resulting from them shall explicitly stipulate that the Court of Auditors and OLAF shall carry



out, if necessary, on-the-spot checks among the recipients of the Agency's funding and the agents responsible for allocating it.

### 13. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

#### 13.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

– Existing expenditure budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Description.....]	Diff./non-diff. (1)	from EFTA <sup>2</sup> countries	from candidate countries <sup>3</sup>	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation
3A	18.02.11.01  Agency for the operational management of large-scale IT systems in the area of freedom, security and justice — Contribution to Titles 1 and 2	DA	NO	NO	YES	NO
	18.02.11.02  Agency for the operational management of large-scale IT systems in the area of freedom, security and justice — Contribution to Title 3					

– New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Heading.....]	Diff./non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation
	[XX.YY.YY.YY]		YES/ NO	YES/ NO	YES/ NO	YES/NO

<sup>1</sup> Diff. = Differentiated appropriations / Non-Diff. = Non-differentiated appropriations

<sup>2</sup> EFTA: European Free Trade Association.

<sup>3</sup> Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

## 13.2. Estimated impact on expenditure

### 13.2.1. Summary of estimated impact on expenditure

EUR million (to 3 decimal places)

<b>Heading of multiannual financial framework:</b>	Number	[Heading 3A]
--	--------	--------------

DG: <Home Affairs>			Year	Year	Year	... enter as many years as necessary to show the duration of the impact (see point 1.6)			<b>TOTAL</b>
			N <sup>1</sup> (2013)	N+1	N+2				
Title 1 (Human Resources) <sup>2</sup>	Commitments	(1)	0.128	0.064	0.064				<b>0.256</b>
	Payments	(2)	0.128	0.064	0.064				<b>0.256</b>
Title 2 (Other Administrative Expenditure) <sup>3</sup>	Commitments	(1a)	0.100	0	0				<b>0.100</b>
	Payments	(2a)	0.100	0	0				<b>0.100</b>
Title 3 (Operational Expenditure)	Commitments	(3a)	2.415	0	0				<b>2.415</b>
	Payments	(3b)	1.690	0.725	0				<b>2.415</b>
<b>TOTAL appropriations for DG &lt;Home Affairs&gt;</b>	Commitments	=1+1a +3a	2.643	0.064	0.064				<b>2.771</b>
	Payments	=2+2a +3b	1.918	0.789	0.064				<b>2.771</b>

<sup>1</sup> Year N is the year in which implementation of the proposal/initiative starts.

<sup>2</sup> See 13.2.3.1 for explanation of HR costs

<sup>3</sup> Conferences, meetings, other administrative expenses.

<b>Heading of multiannual financial framework:</b>	<b>5</b>	" Administrative expenditure "
--	----------	--------------------------------

EUR million (to 3 decimal places)

		Year N	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
DG: <Home Affairs>									
• Human resources		0	0	0					
• Other administrative expenditure		0	0	0					
<b>TOTAL DG &lt;Home Affairs&gt;</b>	Appropriations	0	0	0					

<b>TOTAL appropriations under HEADING 5 of the multiannual financial framework</b>	(Total commitments = Total payments)	0	0	0					
--	--------------------------------------	---	---	---	--	--	--	--	--

EUR million (to 3 decimal places)

		Year N <sup>1</sup>	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
<b>TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework</b>	Commitments	2.643	0.064	0.064					2.771
	Payments	1.918	0.789	0.064					2.771

<sup>1</sup> Year N is the year in which implementation of the proposal/initiative starts.

### 13.2.2. Estimated impact on [body] appropriations

- The proposal/initiative does not require the use of operational appropriations
- The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to 3 decimal places)

Indicate objectives and outputs  ↓	... enter as many years as necessary to show the duration of the impact (see point 1.6)																TOTAL	
	OUTPUTS																	
	Type of output <sup>1</sup>	Average cost of the output	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Number of outputs	Cost	Total number of outputs	Total cost
SPECIFIC OBJECTIVE No 1 <sup>2</sup> Asylum Requirements deriving from the EURODAC Regulation																		
Changes other than for Law Enforcement Access	Imple		1	0.100	0	0	0	0	0	0								0.100
Sub-total for specific objective N°1			1	0.100	0	0	0	0	0	0								0.100
SPECIFIC OBJECTIVE No 2 facilitate prevention, detection and investigation of terrorist offences and other serious criminal offences																		
Changes for Law Enforcement Access	Imple		1	2.543	1	0.064	1	0.064										2.671
Sub-total for specific objective N°2			1	2.543	1	0.064	1	0.064										2.671

<sup>1</sup> Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

<sup>2</sup> As described in Section 1.4.2. "Specific objective(s)..."

**TOTAL COST**

**2 2.643 1 0.064 1 0.064**

**2.771**

### 13.2.3. Estimated impact on the IT Agency's human resources

#### 13.2.3.1. Summary

- The proposal/initiative does not require the use of appropriations of an administrative nature
- The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to 3 decimal places)

	Year N <sup>1</sup>	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)	TOTAL
--	---------------------	----------	----------	----------	---	-------

Officials (AD Grades)							
Officials (AST grades)							
Contractual agent	0.128	0.064	0.064				<b>0.256</b>
Temporary agents							
Seconded National Experts							

<b>TOTAL</b>	<b>0.128</b>	<b>0.064</b>	<b>0.064</b>				<b>0.256</b>
--------------	--------------	--------------	--------------	--	--	--	--------------

Annual Human Resources Requirements	N	N+1	N+2
Total number of Human Resources	2	1	1

Existing IT Agency staff cannot be used for the upgrade of EURODAC because they are not development staff and are needed to operate the existing EURODAC functionalities. The changes provided by this Recast to permit the comparison of latent fingerprints from a crime-scene with live rolled fingerprints require expertise that the IT Agency and currently the Commission do not possess. As such, it will be necessary to hire contractual agents as follows:

Year N: Two contractual agents required to work the on technical tasks (technical specifications, technical support to the administrative tasks, coordination of internal services) as well as on the call for tender preparation and publication, opening

<sup>1</sup> Year N is the year in which implementation of the proposal/initiative starts.

committee, evaluation committee, evaluation report, award decision, contract signature).

In years N+1 and N+2, one staff member would be needed for technical tasks (project management, follow-up of contract deliverables, deliverable quality check and acceptance, coordination of internal services, service orders, change requests).

By year N+3 the new functionalities will become operational once the development phase is complete and as such no additional staff should be required.



### 13.2.3.2. Estimated requirements of human resources for the parent DG

- The proposal/initiative does not require the use of human resources
- The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full amounts (or at most to one decimal place)

	Year N	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)		
<b>• Establishment plan posts (officials and temporary agents)</b>							
XX 01 01 01 (Headquarters and Commission's Representation Offices)							
XX 01 01 02 (Delegations)							
XX 01 05 01 (Indirect research)							
10 01 05 01 (Direct research)							
<b>• External personnel (in Full Time Equivalent unit: FTE)<sup>1</sup></b>							
XX 01 02 01 (CA, INT, SNE from the "global envelope")							
XX 01 02 02 (CA, INT, JED, LA and SNE in the delegations)							
XX 01 04 <i>yy</i> <sup>2</sup>	- at Headquarters <sup>3</sup>						
	- in delegations						
XX 01 05 02 (CA, INT, SNE - Indirect research)							
10 01 05 02 (CA, INT, SNE - Direct research)							

<sup>1</sup> CA= Contract Agent; INT= agency staff ("*Intérimaire*"); JED= "*Jeune Expert en Délégation*" (Young Experts in Delegations); LA= Local Agent; SNE= Seconded National Expert;

<sup>2</sup> Under the ceiling for external personnel from operational appropriations (former "BA" lines).

<sup>3</sup> Essentially for Structural Funds, European Agricultural Fund for Rural Development (EAFRD) and European Fisheries Fund (EFF).

Other budget lines (specify)							
<b>TOTAL</b>							

**XX** is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary agents	
External personnel	

Description of the calculation of cost for FTE equivalent should be included in the Annex, section 3.

### 13.2.4. Compatibility with the current multiannual financial framework

- Proposal/initiative is compatible with both the 2007-13 and 2014-20 multiannual financial frameworks.
- Proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts.

- Proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework<sup>1</sup>.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

### 13.2.5. Third-party contributions

- The proposal/initiative does not provide for co-financing by third parties
- The proposal/initiative provides for the co-financing estimated below:

Appropriations in EUR million (to 3 decimal places)

	Year N	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
<i>Specify the co-financing body</i>								
TOTAL appropriations cofinanced								

<sup>1</sup> See points 19 and 24 of the Interinstitutional Agreement.

### 13.3. Estimated impact on revenue

–  Proposal/initiative has no financial impact on revenue.

–  Proposal/initiative has the following financial impact:

on own resources

(1)  on miscellaneous revenue

EUR million (to 3 decimal places)

Budget revenue line:	Appropriations available for the ongoing budget year	Impact of the proposal/initiative <sup>1</sup>							
		Year N	Year N+1	Year N+2	Year N+3	... insert as many columns as necessary in order to reflect the duration of the impact (see point 1.6)			

For miscellaneous assigned revenue, specify the budget expenditure line(s) affected.

Revenue line 6312

Specify the method for calculating the impact on revenue.

[NO, IS, CH and FL contribute for a total of 12.452% in the payments made over a given year]

<sup>1</sup> As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 25% for collection costs.