Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

REGULATION (EU) No 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 26 June 2013

on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 78 (2)(e), 87(2)(a) and 88(2)(a) thereof,

Having regard to the proposal from the European Commission

Having regard to the opinion of the European Data Protection Supervisor[(1)],

Acting in accordance with the ordinary legislative procedure[(2)],

Whereas:

(1) A number of substantive changes are to be made to Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention[(3)] and to 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[(4)]. In the interest of clarity, those Regulations should be recast.

(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an

area of freedom, security and justice open to those who, forced by circumstances, seek international protection in the Union.

(3) The European Council of 4 November 2004 adopted The Hague Programme which set 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 procedure comprising common guarantees and a uniform status for refugees and for persons eligible for subsidiary protection.

(4) For the purposes of applying Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person[(5)], it is necessary to establish the identity of applicants for international protection and of persons apprehended in connection with the unlawful crossing of the external borders of the Union. It is also desirable, in order effectively to apply Regulation (EU) No 604/2013, and in particular Article 18(1)(b) and (d) thereof, to allow each Member State to check whether a third-country national or stateless person found illegally staying on its territory has applied for international protection in another Member State.

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

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

(7) The Hague Programme called for the improvement of access to existing data filing systems in the 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 the prevention, detection or investigation of terrorist offences as referred to in Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism[(6)] or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States[(7)]. 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 the European Police Office (Europol).

(9) The powers granted to law enforcement authorities to access Eurodac should be without prejudice to the right of an applicant for international protection to have his or her

application processed in due course in accordance with the relevant law. Furthermore, any subsequent follow-up after obtaining a 'hit' from Eurodac should also be without prejudice to that right.

(10) The Commission outlines in its Communication to the Council and the European Parliament of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs that authorities responsible for internal security could have access to Eurodac in well defined cases, when there is a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for international protection. In that Communication the Commission also found that the proportionality principle requires that Eurodac be queried for such purposes only if 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.

(11) Moreover, Europol plays 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 within the framework of its tasks and in accordance with Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol)[(8)].

(12) Requests for comparison of Eurodac data by Europol should be allowed only in specific cases, under specific circumstances and under strict conditions.

(13) Since Eurodac was originally established to facilitate the application of the Dublin Convention, access to Eurodac for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes a change of the original purpose of Eurodac, which interferes with the fundamental right to respect for 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 protect a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.

(14) Even though the original purpose of the establishment of Eurodac did not require the facility of requesting comparisons of data with the database on the basis of a latent fingerprint, which is the dactyloscopic trace which may be found at a crime scene, such a facility is fundamental in the field of police cooperation. The possibility to compare a latent fingerprint with the fingerprint data which is stored in Eurodac in cases where there are reasonable grounds for believing that the perpetrator or victim may fall under one of the categories covered by this Regulation will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting or investigating

terrorist offences or other serious criminal offences, when for example the only evidence available at a crime scene are latent fingerprints.

(15) 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 or 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. The strictness of those conditions reflects the fact that the Eurodac database registers fingerprint data of persons who are not presumed to have committed a terrorist offence or other serious criminal offence.

(16) With a view to ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with the current Union asylum acquis, in particular with Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted[9] and Regulation (EU) No 604/2013, it is appropriate to extend the scope of this Regulation in order to include applicants for subsidiary protection and persons eligible for subsidiary protection.

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

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

(19) Member States should ensure the transmission of fingerprint data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. All authorities with a right of access to Eurodac should invest in adequate training and in the necessary technological equipment. The authorities with a right of access to Eurodac should inform the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council[10] (the "Agency") of specific difficulties encountered with regard to the quality of data, in order to resolve them.

(20) The fact that it is temporarily or permanently impossible to take and/or to transmit fingerprint data, due to reasons such as insufficient quality of the data for appropriate comparison, technical problems, reasons linked to the protection of health or due to the data subject being unfit or unable to have his or her fingerprints taken owing to

circumstances beyond his or her control, should not adversely affect the examination of or the decision on the application for international protection lodged by that person.

(21) Hits obtained from Eurodac should be verified by a trained fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No 604/2013 and the exact identification of the criminal suspect or victim of crime whose data might be stored in Eurodac.

(22) Third-country nationals or stateless persons who have requested international protection in one Member State may have the option of requesting international protection in another Member State for many years to come. Therefore, the maximum period during which fingerprint data should be kept by the Central System should be of considerable length. Given that most third-country nationals or stateless persons who have stayed in the 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 storage of fingerprint data.

(23) The storage period should be shorter in certain special situations where there is no need to keep fingerprint data for that length of time. Fingerprint data should be erased immediately once third-country nationals or stateless persons obtain citizenship of a Member State.

(24) 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.

(25) 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 took up its responsibilities on 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 or investigation of terrorist offences or 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.

(26) 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 of the Council[(11)] (together referred to as the 'Staff Regulations') should apply to all staff working in the Agency on matters pertaining to this Regulation.

(27) It is necessary to lay down clearly the respective responsibilities of the Commission and the Agency, in respect of the Central System and the Communication Infrastructure, and

of the Member States, as regards data processing, data security, access to, and correction of, recorded data.

(28) It is necessary to designate the competent authorities of the Member States as well as the National Access Point through which the requests for comparison with Eurodac data are made 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 or investigation of terrorist offences or of other serious criminal offences.

(29) Requests for comparison with data stored in the Central System should be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and should be reasoned. The operating units within the designated authorities that are authorised to request comparisons with Eurodac data should not act as a verifying authority. The verifying authorities should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request, without forwarding the reasons for it, for comparison through the National Access Point to the Central System following verification that all conditions for access are fulfilled. In exceptional cases of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the verifying authority should process the request immediately and only carry out the verification afterwards.

(30) The designated authority and the verifying authority may be part of the same organisation, if permitted under national law, but the verifying authority should act independently when performing its tasks under this Regulation.

(31) 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 in specific cases and when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. 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 offence or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that they will commit or have committed any such offence. A specific case also exists when the request for comparison is connected to a person who is the victim of a terrorist offence 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 offence or other serious criminal offence.

(32) In addition, access should be allowed only on condition that comparisons with the national fingerprint databases of the Member State and with the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime[12] did not lead to the

establishment of the identity of the data subject. That condition requires the requesting Member State to conduct comparisons with the automated fingerprinting identification systems of all other Member States under Decision 2008/615/JHA which are technically available, unless that Member State can justify that there are reasonable grounds to believe that it would not lead to the establishment of the identity of the data subject. Such reasonable grounds exist in particular where the specific case does not present any operational or investigative link to a given Member State. That condition requires prior legal and technical implementation of Decision 2008/615/JHA by the requesting Member State in the area of fingerprint data, as it should not be permitted to conduct a Eurodac check for law enforcement purposes where those above steps have not been first taken.

(33) Prior to searching Eurodac, designated authorities should also, provided that the conditions for a comparison are met, consult the Visa Information System under Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) 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[(13)].

(34) For the purpose of efficient comparison and exchange of personal data, Member States should fully implement and make use of the existing international agreements as well as of Union law concerning the exchange of personal data already in force, in particular of Decision 2008/615/JHA.

(35) The best interests of the child should be a primary consideration for Member States when applying this Regulation. Where the requesting Member State establishes that Eurodac data pertain 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 applicable to minors and in accordance with the obligation to give primary consideration to the best interests of the child.

(36) While the non-contractual liability of the Union in connection with the operation of the Eurodac system will be governed by the relevant provisions of the Treaty on the Functioning of the European Union (TFEU), 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.

(37) Since the objective of this Regulation, namely the creation of a system for the comparison of fingerprint data to assist the implementation of Union asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(38) 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[(14)] applies to the processing of personal data by the Member

States carried out in application of this Regulation unless such processing is carried out by the designated or verifying authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(39) The processing of personal data by the authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences pursuant to this Regulation should be subject to a standard of protection of personal data under their national law which complies with 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[(15)].

(40) 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.

(41) Transfers of personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System to any third country or international organisation or private entity established in or outside the Union should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to a third country. This implies that Member States should not transfer information obtained from the Central System concerning: the Member State(s) of origin; the place and date of application for international protection; the reference number used by the Member State of origin; the date on which the fingerprints were taken as well as the date on which the Member State(s) transmitted the data to Eurodac; the operator user ID; and any information relating to any transfer of the data subject under Regulation (EU) No 604/2013. That prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No 604/2013 applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

(42) National supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by Decision 2009/371/JHA should monitor the lawfulness of data processing activities performed by Europol.

(43) 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[(16)], and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing, applies 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, bearing in mind that data protection is a key factor in the successful operation of Eurodac and that data security, high technical quality and lawfulness of consultations are essential to ensure the smooth and proper

functioning of Eurodac as well as to facilitate the application of Regulation (EU) No 604/2013.

(44) The data subject should be informed of the purpose for which his or her data will be processed within Eurodac, including a description of the aims of Regulation (EU) No 604/2013, and of the use to which law enforcement authorities may put his or her data.

(45) 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 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.

(46) Member States, the European Parliament, the Council and the Commission should ensure that the national and European supervisory authorities are able to supervise the use of and access to Eurodac data adequately.

(47) It is appropriate to monitor and evaluate the performance of Eurodac at regular intervals, including in terms of whether law enforcement access has led to indirect discrimination against applicants for international protection, as raised in the Commission's evaluation of the compliance of this Regulation with the Charter of Fundamental Rights of the European Union ('the Charter'). The Agency should submit an annual report on the activities of the Central System to the European Parliament and to the Council.

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

(49) It is necessary that Member States be informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No 604/2013.

(50) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter. In particular, this Regulation seeks to ensure full respect for the protection of personal data and for the right to seek international protection, and to promote the application of Articles 8 and 18 of the Charter. This Regulation should therefore be applied accordingly.

(51) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(52) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the TEU and to the TFEU, the United Kingdom has notified its wish to take part in the adoption and application of this Regulation.

(53) In accordance with Article 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the TEU and to the TFEU, 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.

(54) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of Regulation (EU) No 604/2013,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose of "Eurodac"

1 A system known as "Eurodac" is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to Regulation (EU) No 604/2013 for examining an application for international protection lodged in a Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No 604/2013 under the conditions set out in this Regulation.

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 Central System for law enforcement purposes.

3 Without prejudice to the processing of data intended for Eurodac 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 only for the purposes set out in this Regulation and Article 34(1) of Regulation (EU) No 604/2013.

Article 2

Definitions

1 For the purposes of this Regulation:

a 'applicant for international protection' means a third-country national or a stateless person who has made an application for international protection as defined in Article 2(h) of Directive 2011/95/EU in respect of which a final decision has not yet been taken;

b 'Member State of origin' means:

(i) in relation to a person covered by Article 9(1), the Member State which transmits the personal data to the Central System and receives the results of the comparison;

(ii) in relation to a person covered by Article 14(1), the Member State which transmits the personal data to the Central System;

(iii) in relation to a person covered by Article 17(1), the Member State which transmits the personal data to the Central System and receives the results of the comparison;

c 'beneficiary of international protection' means a third-country national or a stateless person who has been granted international protection as defined in Article 2(a) of Directive 2011/95/EU;

d 'hit' means the existence of a match or matches established by the Central System by comparison between fingerprint data recorded in the computerised 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 25(4);

e 'National Access Point' means the designated national system which communicates with the Central System;

f 'Agency' means the Agency established by Regulation (EU) No 1077/2011;

g 'Europol' means the European Police Office established by Decision 2009/371/JHA;

h 'Eurodac data' means all data stored in the Central System in accordance with Article 11 and Article 14(2);

i 'law enforcement' means the prevention, detection or investigation of terrorist offences or of other serious criminal offences;

j 'terrorist offences' means the offences under national law which correspond or are equivalent to those 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 under national law by a custodial sentence or a detention order for a maximum period of at least three years;

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 fingerprint.

2 The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of the Member States for the purposes laid down in Article 1(1) of this Regulation.

3 Unless stated otherwise, the terms defined in Article 2 of Regulation (EU) No 604/2013 shall have the same meaning in this Regulation.

4 The terms defined in Article 2 of Framework Decision 2008/977/JHA shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of the Member States for the purposes laid down in Article 1(2) of this Regulation.

Article 3

System architecture and basic principles

1 Eurodac shall consist of:

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

(i) a Central Unit,

(ii) a Business Continuity Plan and 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.

3 Data on persons covered by Articles 9(1), 14(1) and 17(1) which are processed in the Central System shall be processed on behalf of the Member State of origin under the conditions set out in this Regulation and separated by appropriate technical means.

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

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

Article 4

Operational management

1 The Agency shall be responsible for the operational management of Eurodac.

The 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. A Business Continuity Plan and System shall be developed taking into account maintenance needs and unforeseen downtime of the system, including the impact of business continuity measures on data protection and security.

The Agency shall ensure, in cooperation with the Member States, that at all times the best available and most secure technology and techniques, subject to a cost-benefit analysis, are used for the Central System.

2 The Agency shall 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 tasks relating to the Communication Infrastructure other than those referred to in paragraph 2, in particular:

a the implementation of the budget;

b acquisition and renewal;

c contractual matters.

4 Without prejudice to Article 17 of the Staff Regulations, 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 duties.

Article 5

Member States' designated authorities for law enforcement purposes

1 For the purposes laid down in Article 1(2), Member States shall designate the authorities that are authorised to request comparisons with 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 or of other serious criminal offences. Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security.

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

3 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

Member States' verifying authorities for law enforcement purposes

1 For the purposes laid down in Article 1(2), each Member State shall designate a single national authority or a unit of such an authority 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 or of other serious criminal offences.

The designated authority and the verifying authority may be part of the same organisation, if permitted under national law, but the verifying authority shall act independently when performing its tasks under this Regulation. The verifying authority shall be separate from the operating units referred to in Article 5(3) and shall not receive instructions from them as regards the outcome of the verification.

Member States may designate more than one verifying authority to reflect their organisational and administrative structures, in accordance with their constitutional or legal requirements.

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

Only duly empowered staff of the verifying authority shall be authorised to receive and transmit a request for access to Eurodac in accordance with Article 19.

Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point.

Article 7

Europol

1 For the purposes laid down in Article 1(2), Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority, which shall act independently of the designated authority referred to in paragraph 2 of this Article when performing its tasks under this Regulation and shall not receive instructions from the designated

authority as regards the outcome of the verification. The unit shall ensure that the conditions for requesting comparisons of fingerprints with Eurodac data are fulfilled. Europol 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 For the purposes laid down in Article 1(2), Europol shall designate an operating unit that is authorised to request comparisons with Eurodac data through its designated National Access Point. The designated authority shall be an operating unit of Europol which is competent to collect, store, process, analyse and exchange information to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling within Europol's mandate.

Article 8

Statistics

1 The Agency shall draw up statistics on the work of the Central System every quarter, indicating in particular:

a the number of data sets transmitted on persons referred to in Articles 9(1), 14(1) and 17(1);

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

c the number of hits for persons referred to in Article 14(1) who have subsequently lodged an application for international protection;

d the number of hits for persons referred to in Article 17(1) who had previously lodged an application for international protection in another Member State;

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

f the number of data sets marked, unmarked, blocked and unblocked in accordance with Article 18(1) and (3);

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;

h the number of requests and hits referred to in Article 20(1);

i the number of requests and hits referred to in Article 21(1).

2 At the end of each year, statistical data shall be established in the form of a compilation of the quarterly statistics for that year, including an indication of the number of persons for whom hits have been recorded under paragraph 1(b), (c) and (d). The statistics shall contain a breakdown of data for each Member State. The results shall be made public.

CHAPTER II

APPLICANTS FOR INTERNATIONAL PROTECTION

Article 9

Collection, transmission and comparison of fingerprints

1 Each Member State shall promptly take the fingerprints of all fingers of every applicant for international protection of at least 14 years of age and shall, as soon as possible and no later than 72 hours after the lodging of his or her application for international protection, as defined by Article 20(2) of Regulation (EU) No 604/2013, transmit them together with the data referred to in Article 11(b) to (g) of this Regulation to the Central System.

Non-compliance with the 72-hour time-limit shall 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 the taking of the fingerprints of a quality ensuring appropriate comparison under Article 25, 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 retaken.

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

In the event of serious technical problems, Member States may extend the 72-hour time-limit in paragraph 1 by a maximum of a further 48 hours in order to carry out their national continuity plans.

3 Fingerprint data within the meaning of Article 11(a) transmitted by any Member State, with the exception of those transmitted in accordance with Article 10(b), shall be compared automatically with the fingerprint data transmitted by other Member States and already stored in the Central System.

4 The Central System shall ensure, at 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 System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin. Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 11(a) to (k) along with, where appropriate, the mark referred to in Article 18(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 12 for the purpose of transmission under Article 9(5):

(a) when an applicant for international protection or another person as referred to in Article 18(1)(d) of Regulation (EU) No 604/2013 arrives in the Member State responsible following a transfer pursuant to a decision acceding to a take back request

as referred to in Article 25 thereof, the Member State responsible shall update its data set recorded in conformity with Article 11 of this Regulation relating to the person concerned by adding his or her date of arrival;

(b) when an applicant for international protection arrives in the Member State responsible following a transfer pursuant to a decision acceding to a take charge request according to Article 22 of Regulation (EU) No 604/2013, the Member State responsible shall send a data set recorded in conformity with Article 11 of this Regulation relating to the person concerned and shall include his or her date of arrival;

(c) as soon as the Member State of origin establishes 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 data set recorded in conformity with Article 11 of this Regulation relating to the person concerned by adding the date when that person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of Regulation (EU) No 604/2013;

(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 of this Regulation has left the territory of the Member States in compliance with a return decision or removal order issued following the withdrawal or rejection of the application for international protection as provided for in Article 19(3) of Regulation (EU) No 604/2013, it shall update its data set recorded in conformity with Article 11 of this Regulation relating to the person concerned by adding the date of his or her removal or when he or she left the territory;

(e) the Member State which becomes responsible in accordance with Article 17(1) of Regulation (EU) No 604/2013 shall update its data set recorded in conformity with Article 11 of this Regulation relating to the applicant for international protection by adding the date when the decision to examine the application was taken.

Article 11

Recording of data

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

(a) fingerprint data;

(b) Member State of origin, place and date of the application for international protection; in the cases referred to in Article 10(b), 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 System;

(g) operator user ID;

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

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

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

Article 12

Data storage

1 Each set of data, as referred to in Article 11, shall be stored in the Central System for ten years from the date on which the fingerprints were taken.

2 Upon expiry of the period referred to in paragraph 1, the Central System shall automatically erase the data from the Central System.

Article 13

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 12(1) shall be erased from the Central System in accordance with Article 27(4) as soon as the Member State of origin becomes aware that the person concerned has acquired such citizenship.

2 The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data in accordance with 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 14(1).

CHAPTER III

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

Article 14

Collection and transmission of fingerprint data

1 Each Member State shall promptly take the fingerprints of all fingers of every third-country national or stateless person of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back 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 him or her back.

2 The Member State concerned shall, as soon as possible and no later than 72 hours after the date of apprehension, transmit to the Central System the following data in relation to any 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 System;

g operator user ID.

3 By way of derogation from paragraph 2, the data specified in paragraph 2 relating to persons apprehended as 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 shall be transmitted before their release from custody, confinement or detention.

4 Non-compliance with the 72-hour time-limit referred to in paragraph 2 of this Article shall 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 the taking of fingerprints of a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.

5 By way of derogation from paragraph 1, where it is not possible to take the fingerprints of the apprehended person on account of measures taken to ensure his or her health or the protection of public health, the Member State concerned shall take and send such fingerprints as soon as possible and no later than 48 hours after those health grounds no longer prevail.

In the event of serious technical problems, Member States may extend the 72-hour time-limit in paragraph 2 by a maximum of a further 48 hours in order to carry out their national continuity plans.

Article 15

Recording of data

1 The data referred to in Article 14(2) shall be recorded in the Central System.

Without prejudice to Article 8, data transmitted to the Central System pursuant to Article 14(2) shall be recorded solely for the purposes of comparison with data on applicants for international protection subsequently transmitted to the Central System and for the purposes laid down in Article 1(2).

The Central System shall not compare data transmitted to it pursuant to Article 14(2) with any data previously recorded in the Central System, or with data subsequently transmitted to the Central System pursuant to Article 14(2).

2 As regards the comparison of data on applicants for international protection subsequently transmitted to the Central System with the data referred to in paragraph 1, the procedures provided for in Article 9(3) and (5) and in Article 25(4) shall apply.

Article 16

Storage of data

1 Each set of data relating to a third-country national or stateless person as referred to in Article 14(1) shall be stored in the Central System for 18 months from the date on which his or her fingerprints were taken. Upon expiry of that period, the Central System shall automatically erase such data.

2 The data relating to a third-country national or stateless person as referred to in Article 14(1) shall be erased from the Central System in accordance with Article 28(3) as soon as the Member State of origin becomes aware of one of the following circumstances before the 18 month period referred to in paragraph 1 of this Article has expired:

a the third-country national or stateless person has been issued with a residence document;

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

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

3 The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data for the reason specified in paragraph 2(a) or (b) of this Article 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, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data for the reason specified in paragraph 2(c) of this Article 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 14(1).

CHAPTER IV

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

Article 17

Comparison of fingerprint data

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

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

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

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

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

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

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

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

4 Once the results of the comparison of fingerprint data have been transmitted to the Member State of origin, the record of the search shall be kept by the Central System only for the purposes of Article 28. Other than for those purposes, no other record of the search may be stored either by Member States or by the Central System.

5 As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for international protection transmitted by other Member States which have already been stored in the Central System, the procedures provided for in Article 9(3) and (5) and in Article 25(4) shall apply.

CHAPTER V

BENEFICIARIES OF INTERNATIONAL PROTECTION

Article 18

Marking of data

1 For the purposes laid down in Article 1(1), the Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded in the Central System pursuant to Article 11 shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. That mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5). The Central System shall inform all Member States of origin of the marking of data 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 14(1). Those Member States of origin shall also mark the corresponding data sets.

2 The data of beneficiaries of international protection stored in the Central System and marked pursuant to paragraph 1 of this Article shall be made available for comparison for the purposes laid down in Article 1(2) for a period of three years after the date on which the data subject was granted international protection.

Where there is a hit, the Central System shall transmit the data referred to in Article 11(a) to (k) for all the data sets corresponding to the hit. The Central System shall not transmit the mark referred to in paragraph 1 of this Article. Upon the expiry of the period of three years, the Central System shall automatically block such data from being transmitted in the event of a request for comparison for the purposes laid down in Article 1(2), whilst leaving those data available for comparison for the purposes laid down in Article 1(1) until the point of their erasure. Blocked data shall not be transmitted, and the Central System shall return a negative result to the requesting Member State in the event of a hit.

3 The Member State of origin shall unmark or unblock data concerning a third-country national or stateless person whose data were previously marked or blocked in accordance with paragraphs 1 or 2 of this Article if his or her status is revoked or ended or the renewal of his or her status is refused under Articles 14 or 19 of Directive 2011/95/EU.

CHAPTER VI

PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES

Article 19

Procedure for comparison of fingerprint data with Eurodac data

1 For the purposes laid down in Article 1(2), the designated authorities referred to in Articles 5(1) and 7(2) may submit a reasoned electronic request as provided for in Article 20(1) together with the reference number used by them, to the verifying authority for the transmission for comparison of fingerprint data to the Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether all the conditions for requesting a comparison referred to in Articles 20 or 21, as appropriate, are fulfilled.

2 Where all the conditions for requesting a comparison referred to in Articles 20 or 21 are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the Central System in accordance with Article 9(3) and (5) for the purpose of comparison with the data transmitted to the Central System pursuant to Articles 9(1) and 14(2).

3 In exceptional cases of urgency where there is a need to prevent an imminent danger associated with a terrorist offence or other serious criminal offence, 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 for requesting a comparison referred to in 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 an ex-post verification determines that the access to Eurodac data was not justified, all the authorities that have accessed such data shall erase the information communicated from Eurodac and shall inform the verifying authority of such erasure.

Article 20

Conditions for access to Eurodac by designated authorities

1 For the purposes laid down in Article 1(2), designated authorities may submit a reasoned electronic request for the comparison of fingerprint data with the data stored in the Central System within the scope of their powers only if comparisons with the following databases did not lead to the establishment of the identity of the data subject:

— national fingerprint databases;

— the automated fingerprinting identification systems of all other Member States under Decision 2008/615/JHA where comparisons are technically available, unless there are reasonable grounds to believe that a comparison with such systems would not lead to the establishment of the identity of the data subject. Such reasonable grounds shall be included in the reasoned electronic request for comparison with Eurodac data sent by the designated authority to the verifying authority; and

— the Visa Information System provided that the conditions for such a comparison laid down in Decision 2008/633/JHA are met;

and where the following cumulative conditions are met:

(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, which means that there is an overriding public security concern which makes the searching of the database proportionate;

(b) the comparison is necessary in a specific case (i.e. systematic comparisons shall not be carried out); and

(c) there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. Such reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls in a category covered by this Regulation.

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

Article 21

Conditions for access to Eurodac by Europol

1 For the purposes laid down in Article 1(2), Europol's designated authority may submit a reasoned electronic request for the comparison of fingerprint data with the data stored in the Central System within the limits of Europol's mandate and where necessary for the performance of Europol's tasks only if comparisons with fingerprint data stored in any information processing systems that are technically and legally accessible by Europol did not lead to the establishment of the identity of the data subject and where the following cumulative conditions are met:

a the comparison is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate, which means that there is an overriding public security concern which makes the searching of the database proportionate;

b the comparison is necessary in a specific case (i.e. systematic comparisons shall not be carried out); and

c there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. Such reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls in a category covered by this Regulation.

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 data 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 designated authorities, the verifying authorities and the National Access Points

1 Without prejudice to Article 26, all communication between the designated authorities, the verifying authorities and the National Access Points shall be secure and take place electronically.

2 For the purposes laid down in Article 1(2), fingerprints shall be digitally processed by the Member States 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.

CHAPTER VII

DATA PROCESSING, DATA PROTECTION AND LIABILITY

Article 23

Responsibility for data processing

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 11, Article 14(2) and Article 17(2) are lawfully transmitted to the Central System;

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

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

e the results of fingerprint data comparisons transmitted by the Central System are lawfully processed.

2 In accordance with Article 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 System as well as the security of the data it receives from the Central System.

3 The Member State of origin shall be responsible for the final identification of the data pursuant to Article 25(4).

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

a adopt measures ensuring that persons working with the Central System process the data recorded therein only in accordance with the purposes of Eurodac as laid down in Article 1;

b take the necessary measures to ensure the security of the Central System in accordance with Article 34;

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

The 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.

Article 24

Transmission

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

2 Member States shall transmit the data referred to in Article 11, Article 14(2) and Article 17(2) electronically. The data referred to in Article 11 and Article 14(2) shall be automatically recorded in the Central System. As far as necessary for the efficient operation of the Central System, the Agency shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central System and vice versa.

3 The reference number referred to in Articles 11(d), 14(2)(d), 17(1) and 19(1) 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 a person referred to in Article 9(1), 14(1) or 17(1).

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 or request. "1" refers to data relating to persons referred to in Article 9(1), "2" to persons referred to in Article 14(1), "3" to persons referred to in Article 17(1), "4" to requests referred to in Article 20, "5" to requests referred to in Article 21 and "9" to requests referred to in Article 29.

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

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

Article 25

Carrying out comparisons and transmitting results

1 Member States shall ensure the transmission of fingerprint data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. As far as necessary to ensure that the results of the comparison by the Central System reach a very high level of accuracy, the Agency shall define the appropriate quality of transmitted fingerprint data. The Central System shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data do not lend themselves to comparison using the computerised fingerprint recognition system, the Central System shall inform the Member State concerned. That Member State shall then transmit fingerprint data of the appropriate quality using the same reference number as the previous set of fingerprint data.

2 The Central System shall carry out comparisons in the order of arrival of requests. Each request shall be dealt with within 24 hours. A Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where such time-limits cannot be respected owing to circumstances which are outside the Agency's responsibility, the Central System shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as is necessary for the efficient operation of the Central System, the Agency shall establish criteria to ensure the priority handling of requests.

3 As far as necessary for the efficient operation of the Central System, the Agency shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.

4 The result of the comparison shall be immediately checked in the receiving Member State by a fingerprint expert as defined in accordance with its national rules, specifically trained in the types of fingerprint comparisons provided for in this Regulation. For the purposes laid down in Article 1(1) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned, pursuant to Article 34 of Regulation (EU) No 604/2013.

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

5 Where final identification in accordance with paragraph 4 reveals that the result of the comparison received from the Central System does not correspond to the fingerprint data sent for comparison, Member States shall immediately erase the result of the comparison and communicate this fact as soon as possible and no later than after three working days to the Commission and to the Agency.

Article 26

Communication between Member States and the Central System

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

Article 27

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

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

No Member State may conduct searches of the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in Article 9(5).

2 The authorities of Member States which, pursuant to paragraph 1 of this Article, have access to data recorded in the Central System shall be those designated by each Member State for the purposes laid down in Article 1(1). That 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 units 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 online.

3 Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central System by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article 12(2) or 16(1).

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

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

5 The Agency shall not transfer or make available to the authorities of any third country data recorded in the Central System. This prohibition shall not apply to transfers of such data to third countries to which Regulation (EU) No 604/2013 applies.

Article 28

Keeping of records

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

2 The records referred to in paragraph 1 of this Article 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 34. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year after the storage period referred to in Article 12(1) and in Article 16(1) has expired, unless they are required for monitoring procedures which have already begun.

3 For the purposes laid down in Article 1(1), each Member State shall take the necessary measures in order to achieve the objectives set out in paragraphs 1 and 2 of this Article in relation to its national system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.

Article 29

Rights of the data subject

1 A person covered by Article 9(1), Article 14(1) or Article 17(1) shall be informed by the Member State of origin in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand, of the following:

a the identity of the controller within the meaning of Article 2(d) of Directive 95/46/EC and of his or her representative, if any;

b the purpose for which his or her data will be processed in Eurodac, including a description of the aims of Regulation (EU) No 604/2013, in accordance with Article 4 thereof and an explanation in intelligible form, using clear and plain language, of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;

c the recipients of the data;

d in relation to a person covered by Article 9(1) or 14(1), the obligation to have his or her fingerprints taken;

e the right of access to data relating to him or her, and the right to request that inaccurate data relating to him or her be corrected or that unlawfully processed data relating to him or her 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 30(1).

2 In relation to a person covered by Article 9(1) or 14(1), the information referred to in paragraph 1 of this Article shall be provided at the time when his or her fingerprints are taken.

In relation to a person covered by Article 17(1), the information referred to in paragraph 1 of this Article shall be provided no later than at the time when the data relating to that person are transmitted to the Central System. That obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.

Where a person covered by Article 9(1), Article 14(1) and Article 17(1) is a minor, Member States shall provide the information in an age-appropriate manner.

3 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 Regulation (EU) No 604/2013 shall be drawn up in accordance with the procedure referred to in Article 44(2) of that Regulation.

The leaflet shall be clear and simple, drafted in a language that the person concerned understands or is reasonably supposed to understand.

The leaflet shall be established in such a manner as to enable Member States to complete it with additional Member State-specific information. This Member State-specific information shall include at least the rights of the data subject, the possibility of assistance by the national supervisory authorities, as well as the contact details of the office of the controller and the national supervisory authorities.

4 For the purposes laid down in Article 1(1) of this Regulation, 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 Article 12(a) of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him or her recorded in the Central System and of the Member State which transmitted them to the Central System. Such access to data may be granted only by a Member State.

5 For the purposes laid down in Article 1(1), 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.

6 For the purposes laid down in Article 1(1), 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 which transmitted the data so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the Central System.

7 For the purposes laid down in Article 1(1), if it emerges that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall correct or erase the data in accordance with Article 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 or her.

8 For the purposes laid down in Article 1(1), if the Member State which transmitted the data does not agree that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject without excessive delay why it is not prepared to correct or erase the data.

That Member State shall also provide the data subject with information explaining the steps which he or she can take if he or 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.

9 Any request under paragraphs 4 and 5 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 4 and 5 and shall be erased immediately afterwards.

10 The competent authorities of the Member States shall cooperate actively to enforce promptly the rights laid down in paragraphs 5, 6 and 7.

11 Whenever a person requests data relating to him or her in accordance with paragraph 4, the competent authority shall keep a record in the form of a written document that such a request was made and how it was addressed, and shall make that document available to the national supervisory authorities without delay.

12 For the purposes laid down in Article 1(1) of this Regulation, in each Member State, the national supervisory authority shall, on the basis of his or her request, assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his or her rights.

13 For the purposes laid down in Article 1(1) of this Regulation, 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 or her in exercising his or 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.

14 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 or she is refused the right of access provided for in paragraph 4.

15 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 or her recorded in the Central System, in order to exercise his or her rights under paragraph 5. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject in accordance with paragraph 13 shall subsist throughout the proceedings.

Article 30

Supervision by the national supervisory authorities

1 For the purposes laid down in Article 1(1) of this Regulation, 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 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 with 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 three years. A report of such audit shall be sent to the European Parliament, the Council, the Commission, the Agency, 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 shall, each acting within the scope of their respective competences, cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of Eurodac.

2 Member States shall ensure that every year an audit of the processing of personal data for the purposes laid down in Article 1(2) is carried out by an independent body, in accordance with Article 33(2), including an analysis of a sample of reasoned electronic requests.

The audit shall be attached to the annual report of the Member States referred to in Article 40(7).

3 The national supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their 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.

4 For the purpose laid down in paragraph 3, the national supervisory authorities and the European Data Protection Supervisor shall meet 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 law enforcement purposes

1 Each Member State shall provide that the provisions adopted under national law implementing Framework Decision 2008/977/JHA are also applicable to the processing of personal data by its national authorities for the purposes laid down in Article 1(2) of this Regulation.

2 The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States for the purposes laid down in Article 1(2) of this Regulation, including their transmission to and from Eurodac, shall be carried out by the national supervisory authorities designated pursuant to Framework Decision 2008/977/JHA.

3 The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA and shall be supervised by an independent external data protection supervisor. Articles 30, 31 and 32 of that Decision shall be applicable to the processing of personal data by Europol pursuant to this Regulation. The independent external data protection supervisor shall ensure that the rights of the individual are not violated.

4 Personal data obtained pursuant to this Regulation from Eurodac for the purposes laid down in Article 1(2) shall only be processed for the purposes of the prevention, detection or

investigation of the specific case for which the data have been requested by a Member State or by Europol.

5 The Central System, the designated and verifying authorities and Europol shall keep records of the searches for the purpose of permitting the national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union data protection rules, including for the purpose of maintaining records in order to prepare the annual reports referred to in Article 40(7). Other than for such purposes, personal data, as well as the records of the searches, shall be erased in all national and Europol files after a period of one month, unless the data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol.

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 all data processed by its competent authorities pursuant to this Regulation, adopt the necessary measures, including a security plan, in order to:

a physically protect the 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 purposes 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 IDs 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 those profiles and any other relevant information which those authorities may require for supervisory purposes available to the national supervisory authorities referred to in Article 28 of Directive 95/46/EC and 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 in order to ensure compliance with this Regulation (self-auditing) and to automatically detect within 24 hours any relevant events arising from the application of measures listed in points (b) to (j) that might indicate the occurrence of a security incident.

3 Member States shall inform the Agency of security incidents detected on their systems. The Agency shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents. The Member States concerned, the Agency and Europol shall collaborate during a security incident.

4 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, international organisations or private entities

1 Personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Article 2(b) of Framework Decision 2008/977/JHA.

2 Personal data which originated in a Member State and are exchanged between Member States following a hit obtained for the purposes laid down in Article 1(2) shall not be transferred to third countries if there is a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights.

3 The prohibitions referred to in paragraphs 1 and 2 shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No 604/2013 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 for the purposes laid down in Article 1(2) 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 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 reasonable grounds given not to conduct comparisons with other Member States under Decision 2008/615/JHA, in accordance with Article 20(1) of this Regulation;

c the national file reference;

d the date and exact time of the request for comparison by the National Access Point to the Central System;

e the name of the authority having requested access for comparison, and the person responsible who made the request and processed the data;

f 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;

g the data used for comparison;

h in accordance with national rules or with Decision 2009/371/JHA, the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

3 Logs and documentation shall be used only for monitoring the lawfulness of data processing and for ensuring data integrity and security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 40. 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.

Article 37

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 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 the failure of a Member State to comply with its obligations under this Regulation causes damage to the Central System, that Member State shall be liable for such damage, unless and insofar as the 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 REGULATION (EU) NO 1077/2011

Article 38

Amendments to Regulation (EU) No 1077/2011

Regulation (EU) No 1077/2011 is amended as follows:

(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 it by Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes[17]; and

(b) tasks relating to training on the technical use of Eurodac.;

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

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

(u) adopt the annual report on the activities of the Central System of Eurodac pursuant to Article 40(1) of Regulation (EU) No 603/2013;

(v) make comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013 and ensure appropriate follow-up of those audits;;

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

(x) compile statistics on the work of the Central System of Eurodac pursuant to Article 8(2) of Regulation (EU) No 603/2013;;

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

(z) ensure annual publication of the list of units pursuant to Article 27(2) of Regulation (EU) No 603/2013;;

(3) Article 15(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, or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, 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, Article 26(9) of Regulation (EC) No 767/2008 and Article 4(4) of Regulation (EU) No 603/2013;;

(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 Article 12(1)(t) and the annual report on the activities of the Central System of Eurodac referred to in Article 12(1)(u), on the basis of the results of monitoring and evaluation.;

(5) Article 19(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 Eurodac Advisory Groups..

CHAPTER IX

FINAL PROVISIONS

Article 39

Costs

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

2 The costs incurred by national access points and the costs for connection to the 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 shall be responsible for bearing its costs resulting from requests for comparison with Eurodac data for the purposes laid down in Article 1(2)

Article 40

Annual report: monitoring and evaluation

1 The Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor an annual report on the activities of the Central System, including on its technical functioning and security. The annual report shall include information on the management and performance of Eurodac against pre-defined quantitative indicators for the objectives referred to in paragraph 2.

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

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 By 20 July 2018 and every four years thereafter, the Commission shall produce an overall evaluation of Eurodac, examining the results achieved against objectives and the impact on fundamental rights, including whether law enforcement access has led to indirect discrimination against persons covered by this Regulation, and assessing the continuing validity of the underlying rationale and any implications for future operations, and shall make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

5 Member States shall provide the Agency and the Commission with the information necessary to draft the annual report referred to in paragraph 1.

6 The Agency, Member States and Europol shall provide the Commission with the information necessary to draft the overall evaluation provided for in paragraph 4. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

7 While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with Eurodac data for law enforcement purposes, containing information and statistics on:

— the exact purpose of the comparison, including the type of terrorist offence or serious criminal offence,
— grounds given for reasonable suspicion,
— the reasonable grounds given not to conduct comparison with other Member States under Decision 2008/615/JHA, in accordance with Article 20(1) of this Regulation,
— number of requests for comparison,
— the number and type of cases which have ended in successful identifications, and
— the need and use made of the exceptional case of urgency, including those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority.

Member States' and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.

8 On the basis of Member States and Europol annual reports provided for in paragraph 7 and in addition to the overall evaluation provided for in paragraph 4, the Commission shall compile an annual report on law enforcement access to Eurodac and shall transmit it to the European Parliament, the Council and the European Data Protection Supervisor.

Article 41

Penalties

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

Article 42

Territorial scope

The provisions of this Regulation shall not be applicable to any territory to which Regulation (EU) No 604/2013 does not apply.

Article 43

Notification of designated authorities and verifying authorities

1 By 20 October 2013, each Member State shall notify the Commission of its designated authorities, of the operating units referred to in Article 5(3) and of its verifying authority, and shall notify without delay any amendment thereto.

2 By 20 October 2013, Europol shall notify the Commission of its designated authority, of its verifying authority and of the National Access Point which it has designated, and shall notify without delay any amendment thereto.

3 The Commission shall publish the information referred to in paragraphs 1 and 2 in the *Official Journal of the European Union* on an annual basis and via an electronic publication that shall be available online and updated without delay.

Article 44

Transitional provision

Data blocked in the Central System in accordance with Article 12 of Regulation (EC) No 2725/2000 shall be unblocked and marked in accordance with Article 18(1) of this Regulation on 20 July 2015.

Article 45

Repeal

Regulation (EC) No 2725/2000 and Regulation (EC) No 407/2002 are repealed with effect from 20 July 2015.

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

Article 46

Entry into force and applicability

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

This Regulation shall apply from 20 July 2015.

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 20 July 2015.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels, 26 June 2013.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

A. SHATTER

ANNEX I

Data format and fingerprint form

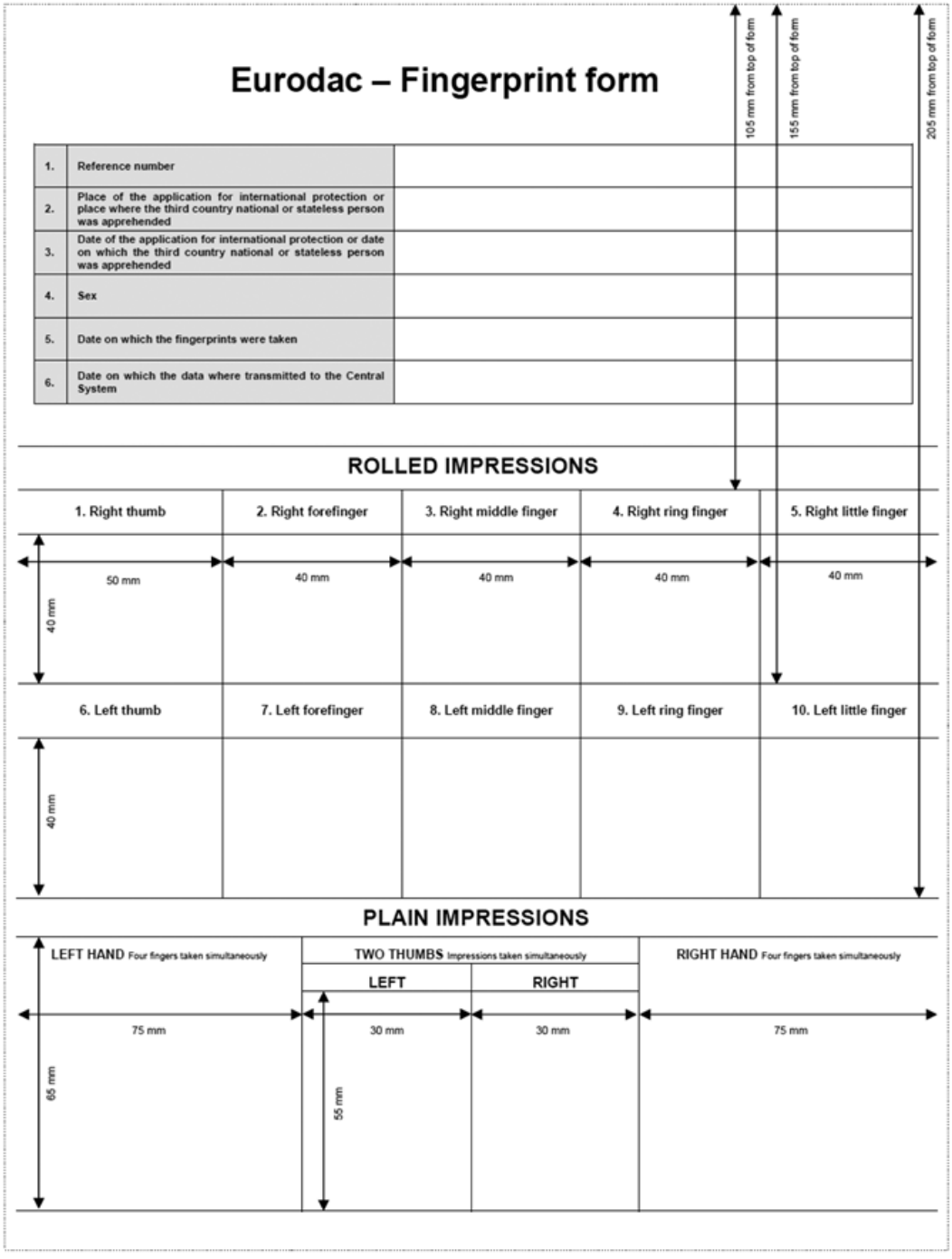
Data format for the exchange of fingerprint data

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

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

Norm for Member State identification letters

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



ANNEX II

REPEALED REGULATIONS (REFERRED TO IN ARTICLE 45)

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

Council Regulation (EC) No 407/2002	(OJ L 62, 5.3.2002 p. 1.)

ANNEX III

CORRELATION TABLE

Regulation (EC) No 2725/2000	**This Regulation**
Article 1(1)	Article 1(1)
Article 1(2), first subparagraph, points (a) and (b)	Article 3(1)(a)
Article 1(2), first subparagraph, point (c)	—
Article 1(2), second subparagraph	Article 3(4)
Article 1(3)	Article 1(3)
Article 2(1)(a)	—
Article 2(1)(b) to (e)	Article 2(1)(a) to (d)
—	Article 2(1)(e) to (j)
Article 3(1)	—
Article 3(2)	Article 3(3)
Article 3(3)(a) to (e)	Article 8(1)(a) to (e)
—	Article 8(1)(f) to (i)
Article 3(4)	—
Article 4(1)	Article 9(1) and Article 3(5)
Article 4(2)	—
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(1), points (a) to (f)	Article 11, points (a) to (f)
—	Article 11, points (g) to (k)
Article 5(1), points (g) and (h)	—
Article 6	Article 12
Article 7	Article 13
Article 8	Article 14
Article 9	Article 15
Article 10	Article 16

Article 11(1) to (3)	Article 17(1) to (3)
Article 11(4)	Article 17(5)
Article 11(5)	Article 17(4)
Article 12	Article 18
Article 13	Article 23
Article 14	—
Article 15	Article 27
Article 16	Article 28(1) and (2)
—	Article 28(3)
Article 17	Article 37
Article 18	Article 29(1), (2), (4) to (10) and (12) to (15)
—	Article 29(3) and (11)
Article 19	Article 30
—	Articles 31 to 36
Article 20	—
Article 21	Article 39(1) and (2)
Article 22	—
Article 23	—
Article 24(1) and (2)	Article 40(1) and (2)
—	Article 40(3) to (8)
Article 25	Article 41
Article 26	Article 42
—	Articles 43 to 45
Article 27	Article 46
Regulation 407/2002/EC	**This Regulation**
Article 2	Article 24
Article 3	Article 25(1) to (3)
—	Article 25(4) and (5)
Article 4	Article 26
Article 5(1)	Article 3(3)
Annex I	Annex I
Annex II	—

(**1**) OJ C 92 10.4.2010, p. 1.

(**2**) Position of the European Parliament of 12 June 2013 (not yet published in the Official Journal) and decision of the Council of 20 June 2013.

(**3**) OJ L 316, 15.12.2000, p. 1.

(**4**) OJ L 62, 5.3.2002, p. 1.

(**5**) See page 31 of this Official Journal.

(**6**) OJ L 164, 22.6.2002, p. 3.

(**7**) OJ L 190, 18.7.2002, p. 1.

(**8**) OJ L 121, 15.5.2009, p. 37.

(**9**) OJ L 337, 20.12.2011, p. 9.

(**10**) OJ L 286, 1.11.2011, p. 1.

(**11**) OJ L 56, 4.3.1968, p. 1.

(**12**) OJ L 210, 6.8.2008, p. 1.

(**13**) OJ L 218, 13.8.2008, p. 129.

(**14**) OJ L 281, 23.11.1995, p. 31.

(**15**) OJ L 350, 30.12.2008, p. 60.

(**16**) OJ L 8, 12.1.2001, p. 1.

(**17**) OJ L 180, 29.6.2013, p. 1.";