Council of the European Union

Brussels, 28 November 2016
(OR. en)

14710/16

Interinstitutional File: 2016/0132 (COD)

LIMITE

ASILE 81
EURODAC 21
ENFOPOL 428
CODEC 1705

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	14462/16 EURODAC 19 CODEC 1665 ENFOPOL 407 ASILE 77
No. Cion doc.:	8765/1/16 ASILE 13 EURODAC 3 ENFOPOL 132 CODEC 630
Subject:	– Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 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] , for identifying an illegally staying third-country national or 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) 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) = Partial general approach

1. On 4 May 2016, the Commission submitted a proposal for a recast of the Eurodac Regulation[1]. The proposal includes the necessary changes to adapt and reinforce the Eurodac system in accordance with the new Dublin rules and to expand its purpose to help tackle irregular migration and facilitate returns.

[1] doc. 8765/1/16 REV 1

2. A detailed examination of the proposal started at the Asylum Working Party on 26 May and continued on 14 June, 14 July and 11 October. The JHA Counsellors examined compromise suggestions from the Presidency at their meetings on 11 and 23 November. The issue of the access of law enforcement authorities to Eurodac has also been discussed at the SCIFA meeting on 13 September, Friends of Presidency meeting on 11 October and by the Council on 13 October 2016.

3. During these discussions, delegations expressed broad support for the proposal to extend its scope by including the possibility for Member States to store and search biometric data belonging to persons who are not applicants for international protection so that they can be identified for return and readmission purposes. The Presidency, considering that a very clear majority supported the text of the proposal and the changes introduced throughout negotiations, considers that the current compromise represents a fair and balanced approach taking into account views expressed by delegations.

4. Given the fact that the recast Eurodac Regulation forms an integral part of the overall reform of the Common European Asylum System (CEAS), cross-references to other parts of the reform package, as well as the provisions relating to the interoperability of information systems, are excluded from the partial general approach and are placed in square brackets. It is also to be understood that it may be necessary to make later some further changes in certain provisions of the Eurodac Regulation to reflect the agreements reached on other proposals currently under discussion, in particular the recast Dublin Regulation.

5. Certain Member States (AT, BE, DE, NL) have requested the inclusion in the Eurodac database of colour copies of travel or identity documents (including a passport photo), if available, in order to facilitate the identification of third-country nationals during the return process. However, since such addition would require additional costs, a cost assessment for the Central System, to be carried out by eu-LISA, is necessary. Once the results of the assessment are known, Member States will be able to consider this issue again. It also has to be born in mind that the costs necessary for upgrading the national systems would not be covered by the assessment and would need to be determined by the Member States themselves.

6. The Presidency invites Coreper to address the following outstanding issues:

a) Conditions for access of law enforcement authorities to Eurodac (recitals 22a, 42, 43, 58 and Articles 6, 9, 19, 21, 22)

While the provisions relating to the law enforcement access have not been amended in the proposal from the Commission, it has been made clear during the examination, including by the Council on 13 October, that Member States are in favour of a simplified and broader access of law enforcement authorities to Eurodac so that the data can be used for the prevention of terrorism and other related security threats in the most efficient way.

On the basis of the replies to the questionnaire circulated by the Presidency[2], amendments have been suggested in the relevant provisions of the Regulation, which aim at simplified and broader access of law enforcement authorities to Eurodac. While the vast majority of delegations supported the suggested changes, a couple of delegations (EE, IT) expressed a preference for the elimination of the obligation to make a prior check in the Prüm system, before law enforcement authorities can access Eurodac. A number of delegations (AT, BE, EE, EL, ES, IE, FI, NL, SE) entered scrutiny reservations on these changes.

The Presidency believes that the changes made in the proposal represent a balanced approach between, on the one hand, the request of the Member States for a broader and simplified access, and, on the other hand, the need for the Council to be able to clearly justify the changes made based on sufficient evidence that they are necessary and proportionate.

The Commission has reserved its position pending the outcome of the discussions within the Council and at the European Parliament.

[2] 13035/16 and 14099/16

b) Comparison of biometric data (Articles 15, 16, 26(5) and recital 31)

The proposal for the recast Eurodac Regulation introduced the obligation for Member States to take, alongside fingerprints, also facial image of the persons concerned. The issues relating to the accuracy of the facial image comparison, the technical standards for the facial image and the associated costs for Member States after adding the facial recognition software have been subject of repeated discussions at experts level. It has been recalled that the technical study to be carried out by eu-LISA in accordance with Art. 42(4) will look into all these aspects. Commission services provided clarifications on the possibilities for Member States to benefit from EU funds as regards the necessary future investments at the national level stemming from the recast Eurodac proposal[3]. Some delegations have also requested that the results of facial image comparison should be verified by experts (Art. 26(5)). To address these concerns, new text has been added in recital 31, which was positively received by the vast majority of delegations. A further minor suggestion is being proposed in the current text. Following these adjustments, the Presidency considers that the compromise, as presented in Annex I to this note, could be agreed upon by delegations. Delegations having scrutiny reservations (CZ, DE, RO, SE) are invited to lift these.

d) Other issues

– DE and FR delegations have expressed preference for an automatic comparison of fingerprints rather than verification of the results of comparison by experts (Art. 26(4)). However, this provision has remained unchanged in the Commission's proposal. Given that the Commission has opposed such change, the Presidency considers that the text should not be amended.

[3] WK 795/16

– AT, DE and FR delegations have suggested that it should be possible to make searches in the Eurodac database on the basis of alphanumeric data in order to enhance the security of the Schengen area. This issue has been analysed in detail at expert meetings as well as bilaterally with the delegations concerned and explanations were provided as to whether this is not feasible. In particular, it has been recalled that Eurodac is a biometric matching database and not a casework system and the accuracy of results would be at stake if such changes were introduced. Data protection and financial concerns were also underlined. Based on this, the Presidency considers that the text should not be changed.

– DE delegation considered that a consultation procedure, similar to the visa consultation procedure under the Visa Code, should be created in Eurodac with a view to improving security in the Schengen area, according to which it should be possible to check at the earliest opportunity the data of persons illegally entering the Schengen area against existing security intelligence of national authorities. The Presidency considers that such procedure should not be introduced in view of the concerns linked to the proportionality of such systematic checks, for reasons of the complexity of the procedure and related costs, as well as technical issues.

7. Some technical changes have been introduced compared to the previous version of the document, notably:

– deletion of Art. 14(3), which is no longer relevant and is entirely covered by Art. 15;
– reference to the opinion of the European Economic and Social Committee has been added;
– in recital 42, the text has been aligned with the changes made in Article 21;
– following the notification of the UK on the opt-in to the proposal and information received from IE that it does not intend to take part in the adoption of the Regulation, relevant recitals have been amended accordingly;
– on a suggestion made at the last JHA Counsellors meeting, minor amendments have been made in Art. 10(3), 13(7) and recital 25a.

8. Most delegations still have general scrutiny reservations on the proposal. SI has also a parliamentary reservation and AT and FR have scrutiny reservation on recitals. With a view to reaching an agreement on the text of the draft Regulation, as set out in Annex, the Presidency would like to invite delegations to withdraw these reservations as well as other scrutiny reservations on individual Articles.

9. The changes in the text of the draft Regulation as compared to the Commission proposal are indicated in **bold** and deleted text is marked in […], while amendments with regard to the latest text examined by the JHA Counsellors[4] is indicated by **underlining** the insertion.

10. In view of the above, Coreper is invited to endorse the compromise proposal as set out in Annex to this note with a view to reaching a partial general approach at the Council, granting the Presidency a mandate to start negotiations with the European Parliament. The partial general approach will be agreed upon on the understanding that the parts of the text relating to the other proposals of the CEAS will be revisited once there is an agreement on them. The partial general approach also relates to the issue of interoperability of information systems and the cost assessment mentioned under 5 of the current note.

---

[4] document 14462/16

ANNEX

2016/0132 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment of 'Eurodac' for the comparison of biometric data […] 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], for identifying an illegally staying third-country national or 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), 79(2)(c), 87(2)(a) and 88(2)(a) thereof,

Having regard to the proposal from the European Commission

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee,

Having regard to the opinion of the European Data Protection Supervisor,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) A number of substantive changes are to be made to Regulation (EU) No 603/2013 of the European Parliament and of the Council[5]**.** In the interests of clarity, that Regulation 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) […]

(4) For the purposes of applying Regulation (EU) No […/…] establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, it is 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 […/…], and in particular Articles[..] and [..]) 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 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 (OJ L 180, 29.6.2013, p. 1).

(5) Biometrics 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 **biometric** […] 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 **biometric** […] data, as well as of the electronic means of transmission between the Member States and the Central System, hereinafter the "Communication Infrastructure".

(7) For the purposes of applying and implementing Regulation (EU) No. […/…] it is also necessary to ensure that a separate secure communication infrastructure exists, which Member State's competent authorities for asylum can use for the exchange of information on applicants for international protection. This secure electronic means of transmission shall be known as 'DubliNet' and should be managed and operated by eu-LISA.

(8) […]

(9) In 2015, the refugee and migration crisis brought to the fore challenges faced by some Member States with taking fingerprints of illegally staying third-country nationals or stateless persons who attempted to avoid the procedures for determining the Member State responsible for examining an application for international protection. The Communication of the Commission of 13 May 2015, titled "A European Agenda on Migration"[6] noted that "*Member States must also implement fully the rules on taking migrants' fingerprints at the borders"* and further proposed that *"The Commission will also explore how more biometric identifiers can be used through the Eurodac system (such as using facial recognition techniques through digital photos)*".

[6] COM(2015) 240 final, 13.5.2015

(10) To assist Member States overcome challenges […], where it is impossible to take the fingerprints of the third-country national or stateless person because his or her fingertips are damaged, either intentionally or not, or amputated**, this Regulation also permits the comparison of a facial image without fingerprints**. Member States should exhaust all attempts to ensure that fingerprints can be taken from the data-subject before a comparison using a facial image only can be carried out […].

(11) The return of third-country nationals **or stateless persons** who do not have a right to stay in the Union, in accordance with fundamental rights as general principles of Union law as well as international law, including refugee protection and human rights obligations, and in compliance with the provisions of Directive 2008/115/EC[7], is an essential part of the comprehensive efforts to address migration and, in particular, to reduce and deter irregular migration. To increase the effectiveness of the Union system to return illegally staying third-country nationals **or stateless persons** is needed in order to maintain public trust in the Union migration and asylum system, and should go hand in hand with the efforts to protect those in need of protection.

[7] Directive of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24,12,2008, p. 98.

(12) National authorities in the Member States experience difficulties in identifying illegally staying third-country nationals **or stateless persons** who use deceptive means to avoid their identification and to frustrate the procedures for re-documentation in view of their return and readmission. It is therefore essential to ensure that information on third-country nationals or stateless persons who are found to be staying illegally in the EU are collected and transmitted to Eurodac and are compared also with those collected and transmitted for the purpose of establishing the identity of applicants for international protection and of third-country nationals **or stateless persons** apprehended in connection with the unlawful crossing of the external borders of the Union, in order to facilitate their identification and re-documentation and to ensure their return and readmission, and to reduce identity fraud. It should also contribute to reducing the length of the administrative procedures necessary for ensuring return and readmission of illegally staying third-country nationals **or stateless persons**, including the period during which they may be kept in administrative detention awaiting removal. It should also allow identifying third countries of transit, where the illegally staying third-country national **or stateless person** may be readmitted.

(13) In its Conclusions of 8 October 2015 on the future of return policy, the Council endorsed the initiative announced by the Commission to explore an extension of the scope and purpose of Eurodac to enable the use of data for return purposes[8]. Member States should have the necessary tools at their disposal to be able to detect illegal migration to and secondary movements of illegally staying third-country nationals **or stateless persons** in the Union. Therefore, the data in Eurodac should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of the Member States.

8 EU Action Plan on return, COM(2015) 453 final.

(14) **[**The Commission's Communication on Stronger and Smarter Information Systems for Borders and Security[9] highlights the need to improve the interoperability of information systems as a long-term objective, as also identified by the European Council and the Council. The Communication proposes to set up an Expert Group on Information Systems and Interoperability to address the legal and technical feasibility of achieving interoperability of the information systems for borders and security. This group should assess the necessity and proportionality of establishing interoperability with the Schengen Information **System** (SIS) and the Visa Information **System** (VIS), and examine if there is a need to revise the legal framework for law enforcement access to EURODAC.]

(15) 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[10] or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA[11]. 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).

(16) 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.

---

9 COM(2016) 205 final

10 Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3.

11 Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

(17) The Commission outlined 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.

(18) 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[12].

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

[12] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).

(20) 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. In line with the requirements of Article 52(1) of the Charter of Fundamental Rights of the European Union, 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 to genuinely meet an objective of general interest and proportionate to the legitimate objective it aims to achieve.

(21) 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.

(22) This Regulation also lays down the conditions under which requests for comparison of **biometric** […] 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 **biometric** […] data of persons who are not presumed to have committed a terrorist offence or other serious criminal offence.

(22a) The challenge of maintaining security in an open Europe has been put to a huge test in recent years. In view of the fact that threats are becoming more varied and more international, as well as increasingly cross-border and cross-sectorial in nature, the EU must do its utmost to help Member States protect citizens. Therefore, the expansion of the scope and simplification of law enforcement access to Eurodac should help Member States dealing with the increasingly complicated operational situations and cases involving cross-border crimes and terrorism with direct impact on the security situation in the EU. The conditions of access to Eurodac for the purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences should also allow the law enforcement authorities of the Member States to tackle the cases of suspects using multiple identities. For this purpose, obtaining a hit during a consultation of a relevant database prior to acceding Eurodac should not prevent such access. It may also be a useful tool to respond to the threat from radicalised persons or terrorists who may seek to re-enter the EU under the guise of an asylum-seeker. A broader and simpler access of law enforcement authorities of the Member States to Eurodac may, while guaranteeing the full respect of the fundamental rights, enable Member States to use all existing tools to ensure that people live in an area of freedom, security and justice.

(23) 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[13] and Regulation (EU) No […/…], this Regulation includes applicants for subsidiary protection and persons eligible for subsidiary protection in its scope.

(24) It is also necessary to require the Member States promptly to take and transmit the **biometric** […] 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 or is found to be staying illegally in a Member State, if they are at least six years of age.

(25) In view of strengthening the protection of unaccompanied minors who have not applied for international protection and those children who may become separated from their families, it is also necessary to take **biometric data** […] for storage in the Central System to help establish the identity of a child and assist a Member State to trace any family or links they may have with another Member State. Establishing family links is a key element in restoring family unity and must be closely linked to the determination of the best interests of the child and eventually, the determination of a durable solution.

---

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

(25a) All minors from the age of six years old and above, including unaccompanied minors, should be accompanied at the time their biometric data is being captured for the purposes of Eurodac by a [legal representative] […], guardian or a person trained to safeguard the best interest of the child and his or her general well-being […]. […] The official responsible for taking the biometric data of a minor should also receive training so […] that sufficient care is taken to ensure an adequate quality of fingerprints of the minor and to guarantee that the process is child-friendly so that the minor, particularly a very young minor, feels safe and can readily cooperate with the process for having his or her biometric data […] taken.

(26) The best interests of the minor should be a primary consideration for Member States when applying this Regulation. Where the requesting Member State establishes that Eurodac data pertain to a child, 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.

(27) It is necessary to lay down precise rules for the transmission of such **biometric** […] data to the Central System, the recording of such **biometric** […] data and of other relevant personal data in the Central System, their storage, their comparison with other **biometric** […] 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.

(28) Member States should ensure the transmission of **biometric** […] data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint and facial 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[14] ("eu-LISA") of specific difficulties encountered with regard to the quality of data, in order to resolve them.

(29) The fact that it is temporarily or permanently impossible to take and/or to transmit **biometric** […] 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 **biometric data** […] 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.

(30) Member States should refer to the Commission's Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints **which** […] the Council **invited the Member States to follow** on 20 July 2015[15], which sets out a best practice approach to taking fingerprints of irregular third-country nationals **or stateless persons**. Where a Member State's national law allows for the taking of fingerprints by force or coercion as a last resort, those measures must fully respect the EU Charter of Fundamental Rights. Third-country nationals **or stateless persons** who are deemed to be vulnerable persons and minors should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law. **In this context, detention should only be used as a means of last resort in order to determine or verify a third-country national's or stateless person's identity.**

---

14 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 (OJ L 286, 1.11.2011, p. 1).

15 SWD(2015) 150 final, 27.5.2015

(31) 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 […/…]; the exact identification of the third-country national or stateless person and the exact identification of the criminal suspect or victim of crime whose data might be stored in Eurodac. Hits obtained from Eurodac based on facial images should also be verified **by an** […] **official trained in accordance with national practice, particularly where the comparison is made with a facial image only. Where a fingerprint and facial image comparison is carried out simultaneously and a hit result is received for both biometric data sets, Member States may check and verify the facial image result, if needed** […]**.**

(32) Third-country nationals or stateless persons who have requested international protection in one Member State may try to request international protection in another Member State for many years to come. Therefore, the maximum period during which **biometric** […] 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 **biometric** […] data.

(33) In view of successfully preventing and monitoring unauthorised movements of third-country nationals or stateless persons who have no right to stay in the Union, and of taking the necessary measures for successfully enforcing effective return and readmission to third countries in accordance with Directive 2008/115/EC[16] and the right to protection of personal data, a period of five years should be considered a necessary period for the storage of **biometric** […] data.

[16] OJ L 348, 24.12.2008, p.98

(34) The storage period should be shorter in certain special situations where there is no need to keep **biometric** […] data and all other personal data for that length of time. **Biometric** […] data and all other personal data belonging to a third-country national **or a stateless person** should be erased immediately once third-country nationals or stateless persons obtain citizenship of a Member State.

(35) It is appropriate to store data relating to those data subjects whose **biometric data** […] 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.

(36) eu-LISA 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 eu-LISA took up its responsibilities on 1 December 2012. In addition, Europol should have observer status at the meetings of the Management Board of eu-LISA 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 eu-LISA.

(37) It is necessary to lay down clearly the respective responsibilities of the Commission and eu-LISA, 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.

(38) 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.

(39) 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.

(40) 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.

(41) 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.

(42) In addition, access should be allowed only on condition that **a prior search in** […] the national **biometric** databases of the Member State and **in** […] the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA[17] **has been conducted** […]. 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.

(43) […]

(44) 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.

(45) 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.

[17] 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 (OJ L 210, 6.8.2008, p. 1).

(46) Since the objective of this Regulation, namely the creation of a system for the comparison of **biometric** […] data to assist the implementation of Union asylum and migration 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.

(47) [Directive [2016/…/…] of the European Parliament and of the Council[18]] 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 competent authorities of the Member States for the purposes of the prevention, investigation, detection or prosecution of terrorist offences or of other serious criminal offences including the safeguarding against and the prevention of threats to public security.

(48) The national provisions adopted pursuant to Directive [2016/… /EU] of the European Parliament and of the Council [of … 2016] on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data apply to the processing of personal data by competent authorities of the Member States for the purposes of the prevention, investigation, detection or prosecution of terrorist offences or of other serious criminal offences pursuant to this Regulation.

---

18 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 (OJ L 281, 23.11.1995, p. 31).

(49) The rules set out in Regulation [2016/…/..] regarding the protection of the rights and freedoms of individuals, notably their right to the protection of personal data concerning them , with regard to the processing of personal data should be specified in respect of the responsibility for the processing of the data, of safeguarding the rights of data subjects and of the supervision of data protection, in particular as far as certain sectors are concerned.

(50) 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 name(s); date of birth; nationality; the Member State(s) of origin or Member State of allocation; the details of the identity or travel document; the place and date of application for international protection; the reference number used by the Member State of origin; the date on which the biometric data 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 accordance with Regulation (EU) No **2016/679 and** […] with the national rules adopted pursuant to Directive **2016/680/EU**[…]], in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

(51) In individual cases, information obtained from the Central System may be shared with a third-country in order to assist with the identification of a third-country national **or a stateless person** in relation to his/her return. Sharing of any personal data must be subject to strict conditions. Where such information is shared, no information shall be disclosed to a third-country relating to the fact that an application for international protection has been made by a third-country national **or a stateless person** where the country the individual is being readmitted to, is also the individual's country of origin or another third-country where they will be readmitted. Any transfer of data to a third-country for the identification of a third-country national **or stateless person** must be in accordance with the provisions of Chapter V of Regulation (EU) No. **679/2016** […].

(52) 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.

(53) Regulation (EC) No 45/2001 of the European Parliament and of the Council[19], 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].

[19] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(54) The data subject should be informed in particular of the purpose for which his or her data will be processed within Eurodac, including a description of the aims of Regulation (EU) […/…] , and of the use to which law enforcement authorities may put his or her data.

(55) 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.

(56) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on **21 September 2016**.

(57) 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.

(58) It is appropriate to monitor and evaluate the performance of Eurodac at regular intervals […]. eu-LISA should submit an annual report on the activities of the Central System to the European Parliament and to the Council.

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

(60) 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.

(61) 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.

(62) 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.

(63) […]

(64) […]

(65) […]

(66) […]

(67) [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 Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom has notified, by letter of **17 November 2016**, its wish to take part in the adoption and application of this Regulation.

(68) In accordance with Articles 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 Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(69) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of Regulation (EU) No […/…] ,

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:

   (a) assist in determining which Member State is to be responsible pursuant to Regulation (EU) No […/…] 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 […/…] under the conditions set out in this Regulation;

   (b) assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals **and stateless persons** for determining the appropriate measures to be taken by Member States, including removal and **returns of persons staying illegally** […].

   [(c) lay down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of **biometric** […] data with those stored in the Central System for law enforcement purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.]

2. 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, **biometric** […] data and other personal data may be processed in Eurodac only for the purposes set out in this Regulation and [Article **[32, 33 and 48(1)(b)** […] of Regulation (EU) No 604/2013].

Article 2

Obligation to take biometric data […][20]

1. Member States are obliged to take the **biometric data** […] of persons referred to in Article 10(1), 13(1) and 14(1) for the purposes of Article 1(1)(a) and (b) of this Regulation and shall impose on the data-subject the requirement to provide his or her **biometric data** […] and inform them as such in accordance with Article 30 of this Regulation.

2. Taking **biometric data** […] of minors from the age of six shall be carried out in a child-friendly and child-sensitive manner by officials trained specifically to enrol minor's fingerprints and **to capture** facial images. […] **Minors** shall be accompanied by a responsible adult, guardian or [**legal]** representative at the time their **biometric data** […] are taken. At all times Member States must respect the dignity and physical integrity of the minor during the fingerprinting procedure and when capturing a facial image.

3. Member States **shall** […] introduce administrative sanctions **including the possibility to use means of coercion**, in accordance with their national law, for non-compliance with **providing biometric data** […] in accordance with paragraph 1 of this Article. These sanctions shall be effective, proportionate and dissuasive. […]

20 DE: scrutiny reservation

4. Without prejudice to paragraph 3 of this Article, where enrolment of **biometric data** […] is not possible from third-country nationals **or stateless persons** who are deemed to be vulnerable persons and from a minor due to the conditions of the fingertips or face, the authorities of that Member State shall not use sanctions to coerce the taking of **biometric data** […]. A Member State may attempt to re-take the **biometric data** […] of a minor or vulnerable person who refuses to comply, where the reason for non-compliance is not related to the conditions of the fingertips or facial image or the health of the individual and where it is duly justified to do so. Where a minor, in particular an unaccompanied or separated minor refuses to give their **biometric data** […] and there are reasonable grounds to suspect that there are child safeguarding or protection risks, the minor shall be referred to the national child protection authorities and /or national referral mechanisms.

5. The procedure for taking **biometric data** […] 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 3

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 10(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 13(1), the Member State which transmits the personal data to the Central System and receives the results of the comparison;

(iii) in relation to a person covered by Article 14(1), the Member State which transmits the personal data to the Central System and receives the results of the comparison;

(c) ‘third-country national’ means any person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty and who is not a national of a State which participates in this Regulation by virtue of an agreement with the […] Union;

(d) 'illegal stay' means the presence on the territory of a Member State, of a third-country national **or a stateless person** who does not fulfil, or no longer fulfils the conditions of entry as set out in Article 5 of the Schengen Borders Code or other conditions for entry, stay or residence in that Member State;

(e) '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;

(f) 'hit' means the existence of a match or matches established by the Central System by comparison between **biometric** […] 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 26(4);

(g) 'National Access Point' means the designated national system which communicates with the Central System;

(h) 'eu-LISA' means the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011;

(I) 'Europol' means the European Police Office established by Decision 2009/371/JHA;

(j) 'Eurodac data' means all data stored in the Central System in accordance with Article 12, Article 13(2) and Article 14(2);

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

(l) '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;

(m) '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;

(n) 'fingerprint data' means the data relating to plain and rolled impressions of the fingerprints of all ten fingers, where present, or a latent fingerprint;

(o) 'facial image **data** ' means digital images of the face with sufficient image resolution and quality to be used in automatic biometric matching;

(p) ‘biometric data’ means fingerprint data and facial image data for the purposes of this Regulation;

(q) ‘residence document’ means any authorisation issued by the authorities of a Member State authorising a third-country national or a stateless person to stay on its territory, including the documents substantiating the authorisation to remain on the territory under temporary protection arrangements or until the circumstances preventing a removal order from being carried out no longer apply;

(r) 'Interface Control Document' means the technical document that specifies the necessary requirements to which the National Access Points must adhere, to be able to communicate electronically with the Central system, in particular by detailing the format and possible content of the information exchanged between the Central system and the National Access Points.

2. The terms defined in Article **4 of Regulation (EU) 2016/679** 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)(a) of this Regulation.

3. Unless stated otherwise, the terms defined in Article [..] of Regulation (EU) No […/…] shall have the same meaning in this Regulation.

4. The terms defined in **Article 3** […] of Directive **(EU) 2016/680** […] shall have the same meaning in this Regulation in so far as personal data are processed by the competent authorities of the Member States for the purposes laid down in Article 1(1)(c) of this Regulation.

Article 4

System architecture and basic principles

1. Eurodac shall consist of:

   (a) a […] 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 a secure and encrypted communication channel for Eurodac data ("Communication Infrastructure").

2. The EURODAC Communication Infrastructure will be using the existing 'Secure Trans European Services for Telematics between Administrations' ([…] TESTA **ng**) network. **In order to ensure confidentiality, personal data transmitted to or from Eurodac shall be encrypted.** […]

3. Each Member State shall have a single National Access Point.

4. Data on persons covered by Articles 10(1), 13(1) and 14(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.

5. 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.

Article 5

Operational management

1. eu-LISA 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.

2. eu-LISA 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. Eu-LISA shall be permitted to use real personal data of the Eurodac production system for testing purposes in the following circumstances:

   (a) for diagnostics and repair when faults are discovered with the Central System; and

   (b) for testing new technologies and techniques relevant to enhance the performance of the Central System or transmission of data to it.

   In such cases, the security measures, access control and logging activities at the testing environment shall be equal to the ones for the Eurodac production system. Real personal data adopted for testing shall be rendered anonymous in such a way that the data-subject is no longer identifiable**, where such data can be anonymised**.

3. eu-LISA 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.

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

   (a) the implementation of the budget;

   (b) acquisition and renewal;

   (c) contractual matters.

5. […]

6. Without prejudice to Article 17 of the Staff Regulations, eu-LISA 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 6

Member States' designated authorities for law enforcement purposes

1. For the purposes laid down in Article 1(1)(c), 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. […]

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 7

Member States' verifying authorities for law enforcement purposes

1. For the purposes laid down in Article 1(1)(c), 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 6(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 **biometric data** […] 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 20.

   Only the verifying authority shall be authorised to forward requests for comparison of **biometric data** […] to the National Access Point.

Article 8

Europol

1. For the purposes laid down in Article 1(1)(c), 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 **biometric data** […] 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 **biometric** […] data to the Central System.

2. For the purposes laid down in Article 1 (1)(c), 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 9

Statistics

1. eu-LISA shall draw up statistics on the work of the Central System every month , indicating in particular:

   (a) the number of data sets transmitted on persons referred to in Articles 10(1), 13(1) and 14(1);

   (b) the number of hits for persons referred to in Article 10(1) who have subsequently lodged an application for international protection in another Member State, who were apprehended in connection with the irregular crossing of an external border and who were found illegally staying in a Member State;

   (c) the number of hits for persons referred to in Article 13(1) who have subsequently lodged an application for international protection who were apprehended in connection with the irregular crossing of an external border and who were found illegally staying in a Member State;

   (d) the number of hits for persons referred to in Article 14(1) who had previously lodged an application for international protection in another Member State, who were apprehended in connection with the irregular crossing of an external border and who were found illegally staying in a Member State;

(e) the number of **biometric** […] data which the Central System had to request more than once from the Member States of origin because the **biometric** […] data originally transmitted did not lend themselves to comparison using the computerised fingerprint **and facial image** recognition system;

(f) the number of data sets marked, unmarked, and in accordance with Article 19(1) and **19**[…] (2), (3) and (4);

(g) the number of hits for persons referred to in Article 19(1) and (4) for whom hits have been recorded under points (b), (c) and (d) of this Article;

(h) the number of requests and hits referred to in Article 21(1);

(I) the number of requests and hits referred to in Article 22(1);

(j) the number of requests made for persons referred to in Article 31;

(**k**) […] the number of hits received from the Central System as referred to in Article 26(6).

2. The monthly statistical data for persons referred to in paragraph1(a) to (**k**) […] shall be published and made public by each month. At the end of each year, the yearly statistical data for persons referred to in paragraph 1(a) to (**k**) […] shall be published and made public by eu-LISA. The statistics shall contain a breakdown of data for each Member State.

3. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects **related to the implementation of this Regulation as well as the statistics pursuant to paragraph 1, and make it available upon request to a Member State**.

4. eu-LISA shall establish, implement and host a central repository in its technical sites containing the data referred to in paragraphs 1 to 3, for research and analysis purposes, which would not allow for the identification of individuals and would allow the authorities listed in paragraph 5 to obtain customisable reports and statistics. Access to the central repository shall be granted by means of secured access through the TESTA-ng with control of access and specific user profiles solely for the purpose of reporting and statistics.

5. Access to the central repository shall be granted to eu-LISA, the Commission and to the authorities of Member States, which have been listed as the designated authorities responsible for carrying out tasks related to the application of this Regulation pursuant to Article 28(2). Access may also be granted to authorised users of other Justice and Home Affairs Agencies if access to the data hosted in the central repository is relevant for the implementation of their tasks.

CHAPTER II

APPLICANTS FOR INTERNATIONAL PROTECTION

Article 10

Collection and transmission of fingerprints and facial image data

1. Each Member State shall promptly take the **biometric data** […] of every applicant for international protection of at least six 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 [21(2)]of Regulation (EU) No , transmit them together with the data referred to in Article 12 (c) to (n) 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 **biometric data** […] 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 26, 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 **biometric data** […] 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 **biometric data** […] 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. **Where requested by a Member State <u>concerned</u>, the biometric** […] data may also be taken and transmitted by members of the European Border [and Coast] Guard Teams or by Member State asylum experts when performing tasks and exercising powers in accordance with [Regulation on the European Border [and Coast] Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC] and [Regulation (EU) No. 439/2010].[21]

[21] ES: scrutiny reservation

Article 11

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 17 (1) for the purpose of transmission under Articles 15 and 16 :

(a) when an applicant for international protection or another person as referred to in Article **20** […] (1) (b), (c), (d) or (e) of Regulation (EU) No […/…] arrives in the Member State responsible following a transfer pursuant to a take back notification as referred to in Article 26 thereof, the Member State responsible shall update its data set recorded in conformity with Article 12 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 24 of Regulation (EU) No […/…] , the Member State responsible shall send a data set recorded in conformity with Article 12 of this Regulation relating to the person concerned and shall include his or her date of arrival;

[(c) when an applicant for international protection arrives in the Member State of allocation pursuant to Article **36** […] of Regulation (EU) No. […/…] , that Member State shall send a data set recorded in conformity with Article 12 of this Regulation relating to the person concerned and shall include his or her date of arrival and record that it is the Member State of allocation.]

(d) as soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with Article 12 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, it shall update its data set recorded in conformity with Article 12 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 19(1) of Regulation (EU) No […/…]] shall update its data set recorded in conformity with Article 12 of this Regulation relating to the applicant for international protection by adding the date when the decision to examine the application was taken.

Article 12

Recording of data

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

(a) fingerprint data;

(b) a facial image;

(c) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately;

(d) nationality(is);

(e) place and date of birth;

(f) Member State of origin, place and date of the application for international protection; in the cases referred to in Article 11(b), the date of application shall be the one entered by the Member State who transferred the applicant;

(g) sex;

(h) **where available,** type and number of identity or travel document; three letter code of the issuing country and **expiry date** […];

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

[(j) unique application number of the application for international protection pursuant to Article 22(2) of Regulation (EU) No. […/…];]

[(k) the Member State of allocation in accordance with Article 11(c);]

(l) date on which the **biometric data** […] were taken;

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

(n) operator user ID;

(o) where applicable in accordance with Article 11(a), the date of the arrival of the person concerned after a successful transfer;

(p) where applicable in accordance with Article 11(b), the date of the arrival of the person concerned after a successful transfer;

(q) where applicable in accordance with Article 11(c), the date of the arrival of the person concerned after a successful transfer;

(r) where applicable in accordance with Article 11(d), the date when the person concerned left or was removed from the territory of the Member States;

(s) where applicable in accordance with Article 11(e), the date when the decision to examine the application was taken.

CHAPTER III

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

Article 13

Collection and transmission of biometric […] data[22]

1. Each Member State shall promptly take the **biometric data** […] of every third-country national or stateless person of at least six 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.

[22] SE: scrutiny reservation

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) a facial image;

(c) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately;

(d) nationality(is);

(e) place and date of birth

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

(g) sex;

(h) **where available,** type and number of identity or travel document; three letter code of the issuing country and **expiry date** […];

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

(j) date on which the **biometric data** […] were taken;

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

(l) operator user ID;

(m) where applicable in accordance with paragraph 6, the date when the person concerned left or was removed from the territory of the Member States.

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 **biometric data** […] 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 26, 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 **biometric data** […] 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 **biometric data** […] 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.

6. As soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with paragraph ~~(~~1~~)~~ has left the territory of the Member States in compliance with a return decision or removal order, it shall update its data set recorded in conformity with paragraph 2 relating to the person concerned by adding the date of his or her removal or when he or she left the territory.

7. **Where requested by a Member State concerned, the biometric** […] data may also be taken and transmitted by members of the European Border and Coast Guard Teams when performing tasks and exercising powers in accordance with [Regulation on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC].

CHAPTER IV

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

Article 14

Collection and transmission of biometric […] data[23]

1. Each Member State shall promptly take the **biometric data** […] of every third-country national or stateless person of at least six years of age who is found illegally staying within its territory.

[23] SE: scrutiny reservation

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:

(a) fingerprint data;

(b) a facial image;

(c) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately;

(d) nationality(is);

(e) place and date of birth

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

(g) sex;

(h) **where available,** type and number of identity or travel document; three letter code of the issuing country and **expiry date** […];

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

(j) date on which the **biometric data** […] were taken;

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

(l) operator user ID;

(m) where applicable in accordance with paragraph 6, the date when the person concerned left or was removed from the territory of the Member States

3. […]

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 **biometric data** […] 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 26, 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 **biometric data** […] 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 **biometric data** […] 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.

6. As soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with **paragraph 1** […] has left the territory of the Member States in compliance with a return decision or removal order, it shall update its data set recorded in conformity with paragraph 2 […] relating to the person concerned by adding the date of his or her removal or when he or she left the territory.

CHAPTER V

PROCEDURE FOR COMPARISON OF DATA FOR APPLICANTS FOR INTERNATIONAL PROTECTION AND THIRD-COUNTRY NATIONALS AND STATELESS PERSONS APPREHENDED CROSSING THE BORDER IRREGULARLY OR ILLEGALLY STAYING IN THE TERRITORY OF A MEMBER STATE

Article 15

Comparison of biometric data

1. **Biometric** […] data transmitted by any Member State, with the exception of those transmitted in accordance with Article 11(b) and (c), shall be compared automatically with the **biometric** […] data transmitted by other Member States and already stored in the Central System in accordance with Article 10(1), 13(1) and 14(1).

2. The Central System shall ensure, at the request of a Member State, that the comparison referred to in paragraph 1 of this Article covers the **biometric** […] data previously transmitted by that Member State, in addition to the **biometric** […] data from other Member States.

3. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin following the procedures set out in Article 26(4). Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 12, 13(2) and 14(2) along with, where appropriate, the mark referred to in Article 19(1) and (4). Where a negative […] result is received, the data referred to in Article 12, 13(2) and 14(2) shall not be transmitted.

4. Where […] a hit is received by a Member State from Eurodac that can assist that Member State to carry out its obligations under Article 1(1)(a), that evidence shall take precedence over any other hit received.

Article 16

Comparison of facial image data

(1) Where the condition of the fingertips does not allow for the taking of fingerprints of a quality ensuring appropriate comparison under Article 26 […], a Member State **shall** […] carry out a comparison of facial image data […].

(2) Facial image data and data relating to the sex of the data-subject may be compared automatically with the facial image data and personal data relating to the sex of the data-subject transmitted by other Member States and already stored in the Central System in accordance with Article 10(1), 13(1) and 14(1) with the exception of those transmitted in accordance with Article 11(b) and (c).

(3) The Central System shall ensure, at the request of a Member State that the comparison referred to in paragraph 1 of this Article covers the facial image data previously transmitted by that Member State, in addition to the facial image data from other Member States.

(4) The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin following the procedures set out in Article 26 (**5**) […]. Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 12, 13(2) and 14(2) along with, where appropriate, the mark referred to in Article **19** […] (1) and (4). Where a negative hit result is received, the data referred to in Article 12, 13(2) and 14(2) shall not be transmitted.

(5) Where […] a hit is received by a Member State from Eurodac that can assist that Member State to carry out its obligations under Article 1(1)(a), that evidence shall take precedence over any other hit received.

CHAPTER VI

DATA STORAGE, ADVANCED DATA ERASURE AND MARKING OF DATA

Article 17

Data storage

1. For the purposes laid down in Article 10(1), each set of data relating to an applicant for international protection, as referred to in Article 12, shall be stored in the Central System for ten years from the date on which the **biometric data** […] were taken.

2. For the purposes laid down in Article 13(1), each set of data relating to a third-country national or stateless person as referred to in Article 13(2) shall be stored in the Central System for five years from the date on which his or her **biometric data** […] were taken.

3. For the purposes laid down in Article 14(1), each set of data relating to a third-country national or stateless person as referred to in Article 14(2) shall be stored in the Central System for five years from the date on which his or her **biometric data** […] were taken.

4. Upon expiry of the data storage periods referred to in paragraphs 1 to 3 of this Article, the Central System shall automatically erase the data of the data-subjects from the Central System.

Article 18

Advanced 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 17(1), (2) or (3) shall be erased from the Central System in accordance with Article 28(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 10(1), 13(1) or 14(1).

Article 19

Marking of data[24]

1. For the purposes laid down in Article 1(1)(a), 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 12 shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by eu-LISA. That mark shall be stored in the Central System in accordance with Article 17(1) for the purpose of transmission under Article 15 **and 16**. The Central System shall, as soon as possible and no later than 72 hours, 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 10(1), 13(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(1)(c) **until such data is automatically erased from the Central System in accordance with Article 17(4)** […].

[…]

[24] DE: scrutiny reservation

3. The Member State of origin shall unmark […] data concerning a third-country national or stateless person whose data were previously marked […] 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].

4. For the purposes laid down in Article 1(1)(b), the Member State of origin which granted a residence document to an illegally staying third-country national or stateless person whose data were previously recorded in the Central System pursuant to Article 13(2) and 14(2) shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by eu-LISA. That mark shall be stored in the Central System in accordance with Article 17(2) and (3) for the purpose of transmission under Article 15 and 16. The Central System shall, as soon as possible and no later than 72-hours, 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 Articles 13(1) or 14(1). Those Member States of origin shall also mark the corresponding data sets.

5. The data of illegally staying third-country nationals or stateless persons stored in the Central System and marked pursuant to paragraph 4 of this Article shall be made available for comparison for the purposes laid down in Article 1(1)(c) until such data is automatically erased from the Central System in accordance with Article 17(4).

CHAPTER VII

PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES

Article 20

Procedure for comparison of biometric data with Eurodac data

1. For the purposes laid down in Article 1(1)(c), the designated authorities referred to in Articles 6(1) and 8(2) may submit a reasoned electronic request as provided for in Article 21(1) together with the reference number used by them, to the verifying authority for the transmission for comparison of **biometric data** […] 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 21 or 22, as appropriate, are fulfilled.

2. Where all the conditions for requesting a comparison referred to in Articles 21 or 22 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 Articles 15 and 16 for the purpose of comparison with the **biometric** […] data transmitted to the Central System pursuant to Articles 10(1), 13 (1) and 14(1).

3. A comparison of a facial image with other facial image data in the Central System pursuant to Article 1(1)(c) may be carried out in accordance with Article 16(1), if such data is available at the time the reasoned electronic request is made pursuant to Article 21(1).

4. 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 **biometric** […] 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 21 or Article 22 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.

5. 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 21

Conditions for access to Eurodac by designated authorities

1. For the purposes laid down in Article 1(1)(c), designated authorities may submit a reasoned electronic request for the comparison of **biometric** […] data with the data stored in the Central System within the scope of their powers only if **a prior check has been conducted in** […]:

– national **biometric** […] databases; **and**

– 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 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 **or to specific persons** […]; 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 **biometric** […] data.

Article 22

Conditions for access to Eurodac by Europol

1. For the purposes laid down in Article 1(1)(c), Europol's designated authority may submit a reasoned electronic request for the comparison of **biometric** […] 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 **biometric** […] 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 **or to specific persons** […]; 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 **biometric** […] 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 23

Communication between the designated authorities, the verifying authorities and the National Access Points

1. Without prejudice to Article 27, 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(1)(c), biometric data shall be digitally processed by the Member States and transmitted in the data format as set out in the agreed Interface Control Document, in order to ensure that the comparison can be carried out by means of the computerised fingerprint and facial recognition system.

CHAPTER VIII

DATA PROCESSING, DATA PROTECTION AND LIABILITY[25]

Article 24

Responsibility for data processing

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

   (a) **biometric data** […] and the other data referred to in Article 12, Article 13(2) and Article 14(2) are taken lawfully;

   (b) **biometric** […] data and the other data referred to in Article 12, Article 13(2) and Article 14(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 eu-LISA, data in the Central System are lawfully recorded, stored, corrected and erased;

   (e) the results of **biometric** […] data comparisons transmitted by the Central System are lawfully processed.

2. In accordance with Article 36, 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.

[25] DE: scrutiny reservation

3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article 26(4).

4. eu-LISA shall ensure that the Central System is operated in accordance with the provisions of this Regulation. In particular, eu-LISA 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 36;

   (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.

eu-LISA 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 25

Transmission

1. **Biometric** […] data and other personal data shall be digitally processed and transmitted in the data format as set out in the agreed Interface Control Document. As far as necessary for the efficient operation of the Central System, eu-LISA shall establish the technical requirements for transmission of the data format by Member States to the Central System and vice versa. eu-LISA shall ensure that the **biometric** […] data transmitted by the Member States can be compared by the computerised fingerprint and facial recognition system.

2. Member States shall transmit the data referred to in Article 12, Article 13(2) and Article 14(2) electronically. The data referred to in Article 12, Article 13(2) and Article 14(2) shall be automatically recorded in the Central System. As far as necessary for the efficient operation of the Central System, eu-LISA 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 12(i), 13(2)(i), 14 (2)(i) and 20(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 10(1), 13(1) or 14(1).

4. The reference number shall begin with the identification letter or letters by which 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 10(1), "2" to persons referred to in Article 13(1), "3" to persons referred to in Article 14(1), "4" to requests referred to in Article 21, "5" to requests referred to in Article 22 and "9" to requests referred to in Article 30.

5. eu-LISA 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, eu-LISA shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.

Article 26

Carrying out comparisons and transmitting results

1. Member States shall ensure the transmission of **biometric** […] data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint and facial 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, eu-LISA shall define the appropriate quality of transmitted **biometric** […] data. The Central System shall, as soon as possible, check the quality of the **biometric** […] data transmitted. If **the biometric** […] data do not lend themselves to comparison using the computerised fingerprint and facial recognition system, the Central System shall inform the Member State concerned. That Member State shall then transmit **biometric** […] data of the appropriate quality using the same reference number as the previous set of **biometric** […] 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 eu-LISA'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, eu-LISA shall establish criteria to ensure the priority handling of requests.

3. As far as necessary for the efficient operation of the Central System, eu-LISA 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 of fingerprint data carried out pursuant to Article 15 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. **Where the Central System returns a positive hit result based on fingerprint and facial image data Member States may check and verify the facial image result if needed.** For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.

5. The result of the comparison of facial image data carried out pursuant to Article **15, where a positive hit result based on a facial image is received only, and Article** 16 shall be immediately checked and verified in the receiving Member State. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.

   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.

6. Where final identification in accordance with paragraph 4 **and 5** reveals that the result of the comparison received from the Central System does not correspond to the **biometric** […] 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 eu-LISA and inform them of the reference number of the Member State of origin and the reference number of the Member State that received the result.

Article 27

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, eu-LISA shall establish the technical procedures necessary for the use of the Communication Infrastructure.

Article 28

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 15 and 16.

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)(a) and (b). 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 eu-LISA a list of those units and any amendments thereto. eu-LISA shall publish the consolidated list in the *Official Journal of the European Union*. Where there are amendments thereto, eu-LISA 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 18.

4. If a Member State or eu-LISA has evidence to suggest that data recorded in the Central System are factually inaccurate, it shall, without prejudice to the notification of a personal data breach pursuant to Article [33..] of Regulation (EU) No **2016/679** […], 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 eu-LISA, 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. eu-LISA 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 […/…] applies.

Article 29

Keeping of records

1. eu-LISA 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 17 has expired, unless they are required for monitoring procedures which have already begun.

3. For the purposes laid down in Article 1(1)(a) and (b), 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 30

Rights of information of the data subject

1. **In accordance with Chapter III of Regulation (EU) No. 2016/679, a** […] person covered by Article 10(1), Article 13(1) or Article 14(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 in a concise, transparent, intelligible and easily accessible form, using clear and plain language, of the following:

(a) the identity **and contact details** of the controller within the meaning of Article **4(7)** of **Regulation (EU) No. 2016/679** […] and of his or her representative, if any and the contact details of the data protection officer;

(b) the purpose for which his or her data will be processed in Eurodac **and the legal basis of processing**, including a description of the aims of Regulation (EU) No […/…] , in accordance with Article 6 thereof and an explanation in intelligible form of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;

(c) the recipients or categories of recipients of the data;

(d) in relation to a person covered by Article 10(1) or 13(1) or 14(1), the obligation to have his or her **biometric data** […] taken;

(e) the period for which the data will be stored pursuant to Article 17;

(f) the existence of the right to request from the controller access to data relating to him or her, and the right to request that inaccurate data relating to him or her be rectified and the completion of incomplete personal data or that unlawfully processed personal data concerning him or her be erased or restricted, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the supervisory authorities referred to in Article 32(1);

(g) the right to lodge a complaint to the **national** supervisory authority.

2. In relation to a person covered by Article 10(1) or 13(1) and 14(1), the information referred to in paragraph 1 of this Article shall be provided at the time when his or her **biometric data** […] are taken.

Where a person covered by Article 10(1), Article 13(1) and Article 14(1) is a minor, Member States shall provide the information in an age-appropriate manner **using leaflets and/or infographics and/or demonstrations specifically designed to explain the procedure to capture biometric data to minors**.

3. A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in [Article 6(2)of Regulation (EU) No […/…]] 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 concise, transparent, intelligible and easily accessible form and 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 information by the national supervisory authorities, as well as the contact details of the office of the controller and of the data protection officer, and the national supervisory authorities.

Article 31

Right of access to, rectification and erasure of personal data

1. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, the data subject's rights of access, rectification and erasure shall be exercised in accordance ,with Chapter III **and Articles 77 and 79** of Regulation (EU) No. **2016/679** […] and applied as set out in this Article.

2. The right of access of the data subject in each Member State shall include 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.

2. If the rights of rectification 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.

3. 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 rectify or erase the data in accordance with Article 28(3). That Member State shall confirm in writing to the data subject that it has taken action to correct, rectify, complete, erase or restrict the processing of personal data relating to him or her.

4. 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 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 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.

5. Any request under paragraphs 1 and 2 of this Article for access, rectification or erasure shall contain all the necessary particulars to identify the data subject, including **biometric data** […]. Such data shall be used exclusively to permit the exercise of the data subject's rights referred to in paragraphs 1 and 2 and shall be erased immediately afterwards.

6. The competent authorities of the Member States shall cooperate actively to enforce promptly the data subject's rights for rectification and erasure.

7. Whenever a person requests access to data relating to him or her, 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.

8. 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, where requested, provide information to the data subject concerning the exercise of his or her right to request from the data controller access, rectification, completion, erasure or restriction of the processing of personal data concerning him or her. The supervisory authorities shall cooperate in accordance with Chapter VII of Regulation (EU) **2016/679** […].

Article 32

Supervision by the national supervisory authorities

1. each Member State shall provide that T the **national** supervisory authority or authorities of each Member State […] referred to in Article [**51**[…] (1)] of Regulation (EU) **2016/679** […] shall monitor the lawfulness of the processing of personal data by the Member State in question for the purposes laid out in Article 1(1)(a) and (b), 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 **biometric** […] data.

Article 33

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 eu-LISA, 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 eu-LISA'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, eu-LISA, and the national supervisory authorities. eu-LISA shall be given an opportunity to make comments before the report is adopted.

Article 34

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(1)(c) is carried out by an independent body, in accordance with Article 35(1), 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 42(8).

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 eu-LISA every two years.

Article 35

Protection of personal data for law enforcement purposes

1. The supervisory authority or authorities of each Member State referred to in Article **41(1)** […] of Directive **(EU) 2016/680** […] shall monitor the lawfulness of the processing of personal data under this Regulation by the Member States for the purposes laid down in Article 1(1)(c) of this Regulation, including their transmission to and from Eurodac.

2. 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.

3. Personal data obtained pursuant to this Regulation from Eurodac for the purposes laid down in Article 1(1)(c) 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.

4. Without prejudice to Article [23 and 24] of Directive **(EU) 2016/680**, 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 42(8). 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 36

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 data-processing equipment and national installations in which the Member State carries out operations in accordance with the purposes of Eurodac (equipment, access control and 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 use of automated data-processing systems by unauthorized persons using data communication equipment (user control);

(f) prevent the unauthorised processing of data in Eurodac and any unauthorised modification or erasure of data processed in Eurodac (control of data entry);

(g) 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);

(h) 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 51** […] of Regulation (EU) No. **2016/679**[…]] and in Article 41 of Directive **(EU) 2016/680** […] of without delay at their request (personnel profiles);

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

(j) 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);

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

(l) ensure that installed systems may, in case of interruption, be restored (recovery);

(m) ensure that the functions of Eurodac perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of malfunctioning of the system (integrity);

(n) 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 (k) that might indicate the occurrence of a security incident.

3. Member States shall inform eu-LISA of security incidents detected on their systems without prejudice to the notification and communication of a personal data breach pursuant to [Articles 33 […] and 34 […]] of Regulation (EU) No **2016/679 and Articles 30 and 31 of Directive (EU) 2016/680** […] respectively […]. eu-LISA shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents. The Member States concerned, eu-LISA and Europol shall collaborate during a security incident.

4. eu-LISA 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 37

Prohibition of transfers of data to third countries, international organisations or private entities[26]

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 **3(2)** […] of Directive **(EU) 2016/680** […]].

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(1)(c) shall not be transferred to third countries if there is a real 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. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1) […].

4. The prohibitions referred to in paragraphs 1 and 2 shall be without prejudice to the right of Member States to transfer such data in accordance with Chapter V of Regulation (EU) No **2016/679** […] respectively with the national rules adopted pursuant to **Chapter V of** Directive **(EU) 2016/680** […] to third countries to which Regulation (EU) No […/…] applies.

26 DE: scrutiny reservation

Article 38

Transfer of data to third countries for the purpose of return[27]

1. By way of derogation from Article 37 of this Regulation, the personal data relating to persons referred to in Articles 10(1), 13(2), 14(1) obtained by a Member State following a hit for the purposes laid down in Article 1(1)(a) or (b) may be transferred or made available to a third-country in accordance with **Chapter V** […] of Regulation (EU) No. **2016/679** […], if necessary in order to prove the identity of third-country nationals **or stateless persons** for the purpose of return […].

   […]

   […]

2. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1) […].

3. A third-country shall not have direct access to the Central System to compare or transmit **biometric** […] data or any other personal data of a third-country national or stateless person and shall not be granted access via a Member State's designated National Access Point.

Article 39

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(1)(c) 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.

[27] DE: scrutiny reservation

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 21(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 20(4) 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 which do not contain personal data may be used for the monitoring and evaluation referred to in Article 42. 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 tasks.

Article 40

Liability

1. Any person who, or Member State which, has suffered material or immaterial 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 in any way 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 eu-LISA 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 in accordance with Articles **79 and 80** […] of Regulation (EU) **2016/679** […] and Articles **54 and 55** […] of Directive **(EU) 2016/680** […].

CHAPTER IX

OPERATIONAL MANAGEMENT OF DUBLINET AND AMENDMENTS TO REGULATION (EU) NO 1077/2011[28]

Article 40a

Operational Management of DubliNet and related tasks

1. A separate secure electronic transmission channel between the authorities of Member States known as the 'DubliNet' communication network set-up under [Article 18 of Regulation (EC) No. 1560/2003] for the purposes set out in Articles 32, 33 and 46 of Regulation (EU) No. […/…] shall also be operated and managed by eu-LISA.

2. The operational management of DubliNet shall consist of all the tasks necessary to ensure the availability of DubliNet, five days a week during normal business hours.

3. eu-LISA shall be responsible for the following tasks relating to DubliNet:

(a) technical support to Member States by way of a helpdesk five days a week during normal business hours, including problems relating to communications, email encryption and decryption, and problems arising from signature of forms.

(b) provision of IT security services for DubliNet;

(c) management, registration and renewal of the digital certificates used for encrypting and signing DubliNet e-mail messages;

(d) technical evolution of DubliNet;

(e) contractual matters.

[28] FR: scrutiny reservation

4. 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 DubliNet.

Article 40b

Amendments to Regulation (EU) No 1077/2011

1. In Regulation 1077/2011, Article 1(2) is replaced by the following text:

"2. The Agency shall be responsible for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac and the Entry Exit System (EES).

The Agency shall also be responsible for the operational management of a separate secure electronic transmission channel between the authorities of Member States known as the 'DubliNet' communication network set-up under [Article 18 of Regulation (EC) No. 1560/2003] for the exchange of information under Regulation (EU) No [604/2013]."

2. In Regulation 1077/2011, after Article 5 the following Article is added:

"Article 5c

Tasks relating to DubliNet

1. In relation to DubliNet, the Agency shall perform:

(a) the tasks conferred on it by Regulation (EU) No […/…];

(b) tasks relating to training on the technical use of DubliNet."

CHAPTER IX

FINAL PROVISIONS

Article 41

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(1)(c).

Article 42

Annual report: monitoring and evaluation

1. eu-LISA 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. eu-LISA 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, eu-LISA shall have access to the necessary information relating to the processing operations performed in the Central System.

4. By […] eu-LISA shall conduct a study on the technical feasibility of adding facial recognition software to the Central System for the purposes of comparing facial images. The study shall evaluate the reliability and accuracy of the results produced from facial recognition software for the purposes of EURODAC and shall make any necessary recommendations prior to the introduction of the facial recognition technology to the Central System.

5. By […] 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.

6. Member States shall provide eu-LISA and the Commission with the information necessary to draft the annual report referred to in paragraph 1.

7. eu-LISA, Member States and Europol shall provide the Commission with the information necessary to draft the overall evaluation provided for in paragraph 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

8. 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 **biometric** […] 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 21(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.

9. […]

Article 43

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 44

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 45

Notification of designated authorities and verifying authorities

1. By […], each Member State shall notify the Commission of its designated authorities, of the operating units referred to in Article 6(3) and of its verifying authority, and shall notify without delay any amendment thereto.

2. By […], 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 46

Repeal

Regulation **(EU) No 603/2013 is** repealed with effect from […].

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

Article 47

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 […] [29].

The Interface Control Document shall be agreed between Member States and eu-LISA no later than six months after the entry into force of this Regulation.

[29] 24 months from the date of entry into force of this Regulation.

Articles 2(2), 32 […] and, for the purposes referred to in Article 1(1)(a) and (b), Articles 28(4), 30 and 37 shall apply from the date referred to in Article **99** […] (2) of Regulation (EU) **2016/679** […]. Until this date Articles 2(2), 27(4), 29, 30 and 35 of Regulation 603/2013 shall apply.

Articles 2(4), 35, and for the purposes referred to in Article 1(1)(c), Article 28(4), 30, 37 and 40 shall apply from the date referred to in Article **63** […] (1) of Directive **(EU) 2016/680** […]. Until this date Articles 2(4), 27(4), 29, 33, 35 and 37 of Regulation 603/2013 shall apply.

Comparisons of facial images with the use of facial recognition software as set out in Articles 15 and 16 of this Regulation shall apply from the date upon which the facial recognition technology has been introduced into the Central System. Facial recognition software shall be introduced into the Central System [*two years from the date of entry into force of this Regulation]*. Until that day, facial images shall be stored in the Central System as part of the data-subject's data sets and transmitted to a Member State following the comparison of fingerprints where there is a hit result.

Member States shall notify the Commission and eu-LISA as soon as they have made the technical arrangements to transmit data to the Central System under Articles XX-XX, no later than […].

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*