EUROPEAN
COMMISSION

Brussels, 4.5.2016
COM(2016) 272 final

2016/0132 (COD)

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 (recast)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

EURODAC was established by Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention[1]. A first recast proposal for the amendment of the EURODAC Regulation was adopted by the Council and the European Parliament in June 2013[2], which enhanced the functioning of EURODAC and laid down conditions for law enforcement access to it under strict conditions for the prevention, detection and investigation of serious crimes and terrorist offences.

Since it was established, EURODAC has sufficiently served the purpose of providing fingerprint evidence to assist determine the Member State responsible for examining an asylum application made in the EU. Its primary objective has always been to serve the implementation of Regulation (EU) No. 604/2013[3] (hereafter "the Dublin Regulation") and together these two instruments make up what is commonly referred to as the 'Dublin system'.

When the migration and refugee crisis escalated in 2015, some Member States became overwhelmed with fingerprinting all those who arrived irregularly to the EU at the external borders, and who further transited through the EU en route to their preferred destination. As such, some Member States failed to meet their obligations to take fingerprints under the current EURODAC Regulation. The Communication of the Commission of 13 May 2015, titled "A European Agenda on Migration"[4] noted that "*Member States must also implement fully the rules on taking migrants' fingerprints at the borders"*. This prompted the Commission to bring forward guidance to facilitate systematic fingerprinting, in full respect of fundamental rights, backed up by practical cooperation and exchange of best practices in May 2015.[5] In addition to this the Commission also considered the use of other biometric identifiers to be used for EURODAC, such as facial recognition and the collection of digital photos to counter challenges faced by some Member States to take fingerprints for the purposes of EURODAC.

During the same period, those Member States that are not situated at the external borders began to see an increasing need to be able to store and compare information on irregular migrants that were found illegally staying on their territory, particularly where they did not seek asylum. As a consequence, thousands of migrants remain invisible in Europe, including thousands of unaccompanied minors, a situation that facilitates unauthorised secondary and subsequent movements and illegal stay within the EU. It became clear that significant steps had to be taken to tackle irregular migration that occurred within the EU as well as to the EU.

The Commission's proposal establishing an Entry/Exit System to register entry and exit data of third country nationals crossing the external borders of the EU where a short-stay visa has been obtained for entry to the EU, will allow Member States to detect third-country nationals

---

1 OJ L 062, 05.03.2002, p. 1.
2 OJ L 180, 29.6.2013, p.1
3 OJ L 180, 29.6.2013, p.31
4 COM(2015) 240 final, 13.5.2015
5 Commission Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints, COM(2015) 150 final, 27.5.2015.

who have been staying illegally although they have entered the EU legally.[6] However no such system exists for identifying illegally staying third-country nationals who enter the EU irregularly at the external borders and the current EURODAC system - the ideal database that could host this information - is limited to identifying whether an asylum application has been made in more than one Member State in the EU.

On 6 April 2016, in its Communication "*Towards a reform of the Common European Asylum System and enhancing legal avenues to Europe*"[7] the Commission considered it a priority to bring forward a reform of the Dublin Regulation and establish a sustainable and fair system for determining the Member State responsible for asylum seekers ensuring a high degree of solidarity and a fair sharing of responsibility between Member States by proposing a corrective allocation mechanism. As part of this the Commission considered that EURODAC should be reinforced to reflect changes to the Dublin mechanism and to make sure that it continues to provide the fingerprint evidence it needs to function. It was also considered the EURODAC could contribute to the fight against irregular migration by storing fingerprint data under all categories and allowing comparisons to be made with all stored data for that purpose.

Therefore, this proposal amends the current EURODAC Regulation (EU) No. 603/2013, and extends its scope for the purposes of identifying illegally staying third-country nationals and those who have entered the European Union irregularly at the external borders, with a view to using this information to assist a Member State to re-document a third-country national for return purposes.

Facilitating the identification of illegally staying third-country nationals or stateless persons through the use of biometrics would contribute to improve the effectiveness of the EU return policy, notably in relation to irregular migrants who use deceptive means to avoid their identification and to frustrate re-documentation. The availability of data and information on third-country nationals without any indentification or lawful reason for being in the EU who are fingerprinted in another Member State would accelerate the procedures for the identification and re-documentation of illegally staying third-county nationals apprehended and fingerprinted in another Member State, hence contributing to reduce the length of the necessary return and readmission procedures, including the period during which irregular migrants may be kept in administrative detention awaiting removal, and combat identity fraud. It would allow identifying country of transit of irregular migrants, hence facilitating their readmission in those countries. Furthermore, by providing information on the movements of irregular migrants within the EU, it would allow national authorities to carry out a more accurate individual assessment of the situation of irregular migrants, for instance on the risk that they may abscond, while undertaking return and readmission procedures.

A record number of refugee and migrant children arrived in Europe in 2015 and Member States have struggled to get accurate numbers for unaccompanied and separated children, as formal registration procedures in some Member States do not always allow for their identification when they cross borders. The ongoing migration and refugee crisis has raised profound questions about how to safeguard and protect unaccompanied children by Members of the European Parliament, non-governmental organisations, international organisations and

---

[6] Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011, COM(2016) 194 final, 6.4.2016

[7] COM(2016) 197 final.

Member States. Child protection and missing children from a third-country in particular has become an additional concern of the ensuing crisis within the EU.[8]

Historically, EURODAC has always collected fingerprints of minors from the age of 14 and over, which can allow identification of an unaccompanied minor once an asylum application has been made within the EU. However, given the apparent increase in the smuggling of minors below this age to and within the EU there appears to be a stronger need to collect biometrics for the purposes of EURODAC from a lower age to help with the identification of such persons and to see whether that information can also assist to establish family links or links with a guardian in another Member State.

Many Member States collect biometrics from minors at a younger age than 14 years for visas, passports, biometric residence permits and general immigration control. Thus it is also proposed that the taking of fingerprints of minors for EURODAC should be changed to six years old – the age at which research shows that fingerprint recognition of children can be achieved with a satisfactory level of accuracy.

It will also be necessary to store information on illegally staying third-country nationals and those apprehended entering the EU irregularly at the external border for longer than what is currently permitted. A storage period of 18 months is the maximum permitted under the current Regulation for those apprehended at the external border and no data is retained for those found illegally staying in a Member State. This is because the current EURODAC Regulation is not concerned with storing information on irregular migrants for longer than what it necessary to establish the first country of entry under the Dublin Regulation if an asylum application had been made in a second Member State. Given the extension of the scope of EURODAC for wider migration purposes, it is necessary to retain this data for a longer period so that secondary movements can be adequately monitored within the EU, particularly where an irregular migrant makes all efforts to remain undetected. A period of five years is deemed to be adequate for these purposes, bringing the data retention period in line with other EU databases in the Justice and Home Affairs (JHA) area and the period for which an entry ban can be imposed on an irregular migrant under the Return Directive.[9]

This proposal also allows for information on the identity of an irregular migrant to be shared with a third-country where it is necessary to share that information for return purposes only. The readmission and re-documentation of irregular third-country nationals to their country of origin entails sharing information on that individual with the authorities of that country when a travel document needs to be secured. Thus, this proposal allows data to be shared on that basis and in line with data protection rules. A strict prohibition is set out for sharing any information on the fact that an asylum application has been made within the EU, which could jeopardise a rejected asylum seeker's safety and lead to a violation of his or her fundamental rights.

It is also proposed that an additional biometric – a facial image - will also be collected by Member States and stored in the Central System as well as other personal data to reduce the need for additional communication infrastructure between Member States to share information on irregular migrants that have not claimed asylum. The collection of facial images will be the pre-cursor to introducing facial recognition software in the future and will bring EURODAC in line with the other systems such as the Entry/Exit System. Eu-LISA

---

8 Committee on Civil Liberties, Justice and Home Affairs, Committee Meeting debate, "*Fate of 10,000 missing refugee children",* 21.04.2016

9 OJ L 348, 24.12.2008, p.98

should first conduct a study on facial recognition software that evaluates its accuracy and reliability prior to this software being added to the Central System.

The Commission's Communication on Stronger and Smarter Information Systems for Borders and Security[10] 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 on borders and security. The present proposal is in line with the objectives out in the Communication as it establishes EURODAC in a way that allows for future interoperability with other information systems, where necessary and proportionate. To that end, and with the support of the Expert Group on Information Systems and Interoperability, the Commission will assess the necessity and proportionality of establishing interoperability with the Schengen Information Systems (SIS) and the Visa Information Systems (VIS). In that context, and in line with the Communication, the Commission will also examine if there is a need to revise the legal framework for law enforcement access to EURODAC.

This proposal continues to allow law enforcement access to the Central System and will now permit law enforcement authorities and EUROPOL to have access to all the stored information in the system and to conduct searches based on a facial image in the future.

- **Consistency with other Union policies**

This proposal is closely linked and complements other Union policies, namely:

(a) **The Common European Asylum System** by ensuring the effective implementation of the Dublin Regulation by using fingerprint evidence to assist to determine the Member State responsible for examining an asylum application.

(b) An effective **EU return policy** so as to contribute to and enhance the EU system to return irregular migrants. This is essential for maintaining public trust in the EU's asylum system and support for helping persons in need of international protection. Increasing the rate of return of irregular migrants needs to go hand in hand with the EU's renewed efforts to protect those in need.

(c) **Internal security** as was underlined in the European Agenda on Security[11], to prevent, detect, investigate and prosecute serious crimes and terrorism offences by enabling law enforcement authorities and Europol to process personal data of persons suspected to be involved in acts of terrorism or serious crimes.

(d) **European Border and Coast Guard Teams** as regards the possibility to take and transmit fingerprint and facial image data of asylum applicants and irregular migrants to EURODAC on behalf of a Member State for the effective management of external border control.

(e) **Data Protection** insofar as this proposal must ensure the protection of fundamental rights to respect for the private life of individuals whose personal data are processed in EURODAC.

[10] COM(2016) 205 final
[11] COM(2015) 185 final

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The present recast proposal uses Article 78(2)(e) of the Treaty on the Functioning of the European Union (TFEU) as legal base concerning criteria and mechanisms for determining which Member State is responsible for considering an application for asylum or subsidiary protection, which is the TFEU Article corresponding to the legal base of the original proposal (Article 63(1)(a) of the Treaty establishing the European Community). In addition, it uses Article 79(2)(c) as the legal base concerning the elements of indentifying an irregular third-country national or stateless person as regards illegal immigration and unauthorised residence, including removal and repatriation of persons residing without authorisation, Article 87(2)(a) as the legal base concerning the elements related to the collation, storage, processing, analysis and exchange of relevant information for law enforcement purposes; and Article 88(2)(a) as the legal base concerning Europol's field of action and tasks including the collection, storage, processing, analysis and exchange of information.

• Variable Geometry

The United Kingdom and Ireland are bound by Regulation (EU) No. 603/2013 following their notification of their wish to take part in the adoption and application of that Regulation based on the above-mentioned Protocol.

In accordance with Protocol 21 on the position of the United Kingdom and Ireland, those Member States may decide to take part in the adoption of this proposal. They also have this option after adoption of the proposal.

Under the Protocol on the position of Denmark, annexed to the TEU and the TFEU, Denmark does not take part in the adoption by the Council of the measures pursuant to Title V of the TFEU (with the exception of "measures determining the third countries whose nationals must be in possession of a visa when crossing the external borders of the Member States, or measures relating to a uniform format for visas"). Therefore, Denmark does not take part in the adoption of this Regulation and is not bound by it nor subject to its application. However, given that Denmark applies the current Eurodac Regulation, following an international agreement[12] that it concluded with the EU in 2006, it shall, in accordance with Article 3 of that agreement, notify the Commission of its decision whether or not to implement the content of the amended Regulation.

• Impact of the proposal on non-EU Member States associated to the Dublin system

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

– the agreement associating Iceland and Norway, concluded in 2001[13];

– the agreement associating Switzerland, concluded on 28 February 2008[14];

---

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

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

– the protocol associating Liechtenstein, concluded on 18 June 2011[15].

In order to create rights and obligations between Denmark – which as explained above has been associated to the Dublin/EURODAC acquis via an international agreement – and the associated countries mentioned above, two other instruments have been concluded between the Community and the associated countries.[16]

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

The scope of the above-cited association agreements with Iceland, Norway, Switzerland and Liechtenstein as well as the parallel agreement with Denmark does not cover law enforcement access to EURODAC. Consequently, once this Recast Regulation is adopted it will be necessary to ensure that complementary agreements with those Associated States that wish to participate have been signed and concluded.

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

- **Subsidiarity**

The proposed initiative constitutes a further development of the Dublin Regulation and EU migration policy and in order to ensure that common rules on for the taking of fingerprints and facial image data for irregular third-country nationals for the purposes of EURODAC are applied in the same way in all the Member States. It creates an instrument providing to the European Union information on how many third country nationals enter the EU irregularly and claim asylum, which is indispensable for sustainable and evidence based policy making in

---

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

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

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

the field of migration and visa. It also grants access for law enforcement authorities to EURODAC, which is a timely, accurate, secure and cost-efficient way to identify irregular third-country nationals who are suspects (or victims) of terrorism or of a serious crime.

This proposal will also assist Member States to identify illegally staying third-country nationals and those who have entered the European Union irregularly at the external borders, with a view to using this information to assist a Member State to re-document a third-country national for return purposes.

Due to the transnational nature of the problems related to asylum and refugee protection, the EU is well placed to propose solutions in the framework of the Common European Asylum System (CEAS) to the issues described above as problems regarding the EURODAC Regulation.

An amendment of the EURODAC Regulation is also required in order to add an additional purpose thereto, namely allow access for the purpose to control illegal migration to and secondary movements of irregular migrants within the EU. This objective cannot be sufficiently achieved by the Member States alone.

- **Proportionality**

Article 5 of the Treaty on the European Union states that action by the Union shall not go beyond what is necessary to achieve the objectives of the Treaty. The form chosen for this EU action must enable the proposal to achieve its objective and be implemented as effectively as possible.

The proposal which conception is driven by the *privacy by design* principles is proportionate in terms of the right to protection of personal data in that it does not require the collection and storage of more data for a longer period than is absolutely necessary to allow the system to function and meet its objectives. In addition, all the safeguards and mechanisms required for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data will be foreseen and implemented.

No further processes or harmonisation will be necessary at EU level to make the system work; thus the envisaged measure is proportionate in that it does not go beyond what is necessary in terms of action at EU level to meet the defined objectives.

- **Choice of the instrument**

The proposed recast will also take the form of a Regulation. The present proposal will build on and enhance an existing centralised system through which Member States cooperate with each other, something which requires a common architecture and operating rules. Moreover, it lays down rules on access to the system including for the purpose of law enforcement which are uniform for all Member States. As a consequence, only a Regulation can be chosen as a legal instrument.

3. CONSULTATIONS WITH INTERESTED PARTIES

In preparation of this proposal, the Commission has relied upon the discussions that have been regularly taking place in the European Council and in the Council of Ministers, as well as in the European Parliament on the measures needed to address the migratory crisis and in particular on the reform of the Dublin Regulation, which EURODAC is intrinsically attached to. The Commission has also reflected on the needs of Member States that became apparent during the refugee and migration crisis.

In particular, the Council Conclusions of the European Council of 25-26 June 2015, called for the reinforcement of the management of the Union's external borders to better contain the growing flows of illegal migration.[17] At a further meeting of Heads of State or Government in October 2015, the European Council concluded that Member States needed to step up implementation of the Return Directive and ensure that all those arriving at the hotspots would be identified, registered and fingerprinted and at the same time ensure relocation and returns.[18] In March 2016, the European Council further reiterated that work will also be taken forward on the future architecture of the EU's migration policy, including the Dublin Regulation.[19]

The Commission has also informally consulted the European Data Protection Advisor on the new elements of this proposal that are subject to the new legal framework on Data Protection.

- **Fundamental rights**

The proposed Regulation has an impact on fundamental rights, notably on right to human dignity (Article 1 of the Charter of Fundamental Rights of the EU); the prohibition of slavery and forced labour (Article 5 of the Charter); right to liberty and security (Article 6 of the Charter), respect for private and family life (Article 7 of the Charter), the protection of personal data (Article 8 of the Charter), right to asylum (Article 18 of the Charter) and protection in the event of removal, expulsion or extradition (Article 19 of the Charter), the right to non-discrimination (Article 21 of the Charter), the rights of the child (Article 24 of the Charter) and the right to an effective remedy (Article 47 of the Charter).

The prohibition of slavery and forced labour as well as the right to liberty and security are positively affected by the implementation of EURODAC. A better and more accurate identification (through the use of biometrics) of third-country nationals crossing the external border of the EU supports the detection of identity fraud, human being trafficking (particularly in the case of minors) and cross border criminality and thus contributes to the fight against trafficking and smuggling in human beings. It also contributes to improving the security of the citizens anyone present in the EU area on the EU territory.

The proposal also positively contributes to the protection of the rights of the child and to the respect of the right to respect for family life. Many applicants for international protection and third-country nationals arriving irregularly to the European Union travel with families and in many cases very young children. Being able to identify these children with the help of fingerprints and facial images will help identify children in cases where they are separated from their families by allowing a Member State to follow up a line of inquiry where a fingerprint match indicates that they were present in another Member State. It would also strengthen the protection of unaccompanied minors who do not always formally seek international protection and who abscond from care institutions or child social services under which their care has been assigned.

The obligation to take fingerprints shall be implemented in full respect of the right to human dignity and of the rights of the child. The proposal reaffirms the obligation upon Member States to ensure that the procedure for taking fingerprints and a facial image 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

[17] EUCO 22/15, 26.06.2015
[18] EUCO 26/15, 15.10.2015
[19] EUCO 12/16, 18.03.2016

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. Penalties attached to the failure to comply with the obligation to comply with the fingerprinting process shall be in accordance with the principle of proportionality. In particular, the proposal explicitly states that detention should only be used in this context as a means of last resort if necessary to determine or verify a third-country national's identity. As regards children, the taking of fingerprints from minors, particularly young children, should be carried out in a child-sensitive and child-friendly manner. Relevant provisions also ensure that a child is not subject to any administrative sanctions where there is a justified reason for not submitting their fingerprints or a facial image and that the authorities of a Member State must ensure that where they suspect that there may be child protection issues following a refusal to submit fingerprints or where a child may have damaged fingertips or hands, they should refer the child to the national child protection authorities.

The implementation of the proposal shall be without prejudice to the rights of applicant for and beneficiaries of international protection, in particular as regards the prohibition in the event of removal, expulsion and extradition, including in the context of transfers of personal data to third countries.

As stipulated by Article 52(1) of the Charter, any limitation to the right to the protection of personal data must be appropriate for attaining the objective pursued and not going beyond what is necessary to achieve it. Article 8(2) of the European Convention of Human Rights also recognises that interference by a public authority with a person’s right to privacy may be justified as necessary in the interest of national security, public safety or the prevention of crime, as it is the case in the current proposal. The proposal provides for access to EURODAC for the prevention, detection or investigation of terrorist offences or other serious criminal offences for the purposes of identification of third country nationals crossing the external borders and for the purpose of accessing data on their travel history. Safeguards as regards personal data also include the right of access to or the right of correction or deletion of data. The limitation of the retention period of data referred to above in chapter 1 of this explanatory memorandum also contributes to the respect for personal data as a fundamental right.

The proposal provides for access to EURODAC for the prevention, detection or investigation of terrorist offences or other serious criminal offences for the purposes of identification of third country nationals crossing the external borders and for the purpose of accessing data on their movements within the EU. Moreover, designated law enforcement authorities may only request access to EURODAC data if there are reasonable grounds to consider that such access will substantially contribute to the prevention, detection or investigation of the criminal offence in question. Such requests are verified by a designated law enforcement authority in order to check whether the strict conditions for requesting access to the EES for law enforcement purposes are fulfilled.

Furthermore, the proposal also lays down strict data security measures to ensure the security of personal data processed and establishes supervision of the processing activities by independent public data protection authorities and documentation of all searches conducted. The proposal also states that the processing of all personal data carried out by law enforcement authorities in EURODAC once they have been extracted is subject to the new data protection Directive for the processing of personal data for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties that repeals Council Framework Decision 2008/977/JHA. The proposal establishes strict access

rules to EURODAC and the necessary safeguards. It also foresees the individuals' rights of access, correction, deletion and redresses in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities. Therefore, the proposal fully complies with the Charter of Fundamental Rights of the European Union, in particular as regards the right to the protection of personal data, and is also in line with Article 16 TFEU which guarantees everyone the right to protection of personal data concerning them.

4. BUDGETARY IMPLICATIONS

The present proposal entails a technical amendment to the EURODAC central system in order to provide for the possibility to carry out comparisons for all three categories of data and for storage of all three categories of data. Further functionalities such as the storage of biographical data alongside side a facial image will require more amendments to the Central System

The financial statement attached to this proposal reflects this change.

The cost estimate of 29.872 million EUR includes costs for the technical upgrade and increased storage and throughput of the Central System. It also consists of IT-related services, software and hardware and would cover the upgrade and customisation to allow searches for all categories of data covering both asylum and irregular migration purposes. It also reflects the additional staffing costs required by eu-LISA.

5. OTHER ELEMENTS

- **Detailed explanation of the specific provisions of the proposal**

- Extending the scope of EURODAC for return purposes (Article 1(1)(b)): The scope of the new EURODAC Regulation has been extended to include the possibility for Member States to store and search data belonging to third-country nationals or stateless persons who are not applicants for international protection so that they can be identified for return and readmission purposes. A new legal base, Article 79(2)(c) has been added for these purposes. Thus EURODAC becomes a database for wider immigration purposes and no longer only exists to ensure the effective implementation of the Dublin III Regulation, although this function will still be an important aspect of it. At present EURODAC only compares fingerprint data taken from irregular migrants and applicants for international protection against asylum data because it is an asylum database. Comparisons are not made between fingerprint data taken from irregular migrants at the external borders and fingerprint data taken from third-country nationals found illegally staying on the territory of a Member State.

Extending the scope of EURODAC will allow the competent immigration authorities of a Member State to transmit and compare data on those illegally staying third-country nationals who do not claim asylum and who may move around the European Union undetected. The information obtained in a hit result may then assist competent Member State authorities in their task of identifying illegally staying third-country nationals on their territory for return purposes. It may also provide precious elements of evidence for re-documentation and readmission purposes.

- Ensuring the primacy of the Dublin procedure (Articles 15(4) and 16 (5)): a provision has been included to ensure that where a fingerprint hit indicates that an asylum application has been made in the European Union, the Member State that conducted the search should ensure that the Dublin procedure is followed as a matter of course and not a return procedure for the individual concerned. This is to guarantee that where multiple hits are retrieved from the Central System relating to the same individual, the Member State that consulted EURODAC

is left in no doubt about the correct procedure to follow and so that no applicant for international protection is returned to their country of origin or to a third-country in breach of the principle of *non-refoulement*. Thus the notion of a "hierarchy of hits" has been introduced to allow for this.

- Obligation to take fingerprints and facial images (Article 2): the proposal specifies a clear obligation for Member States to take and transmit fingerprints and a facial image of all three categories of persons and makes sure that Member States impose these obligations on applicants of international protection and third-country nationals or stateless persons so that they are aware. The obligation to take fingerprints has always existed and was communicated to the data-subject via information in the form of a leaflet under Article 29(1)(d) of Regulation (EU) No. 603/2013. This Article also permits Member States to introduce sanctions, in accordance with their national law, for those individuals who refuse to provide a facial imagine or comply with the fingerprinting procedure, following, where relevant, the Commission Staff Working Document on the implementation of the Eurodac Regulation as that sets out a best practice approach for Member States to follow to obtain fingerprints.[20] However, new provisions have been laid down to ensure that the taking of fingerprints and a facial image from minors, particularly young children, should be carried out in a child-sensitive and child-friendly manner. These provisions also ensure that a minor is not subject to any administrative sanctions if they do not submit their fingerprints or a facial image, where there is good reason for not submitting them and that the authorities of a Member State must ensure that where they suspect that there may be child protection issues following a refusal to submit fingerprints or a facial image or where a child may have damaged fingertips or hands, they should refer the child to the national child protection authorities.

- Storing the personal data of the data-subject (Articles 12, 13 and 14): EURODAC has always functioned with fingerprints only and previously no other personal data of the data-subject was stored apart from the gender of the individual. The new proposal now permits the storage of personal data of the data-subject such as the name(s), age, date of birth, nationality, and identity documents, as well as a facial image. The storage of personal data will allow immigration and asylum authorities to easily identify an individual, without the need to request this information directly from another Member State. Personal data of the individual can be retrieved from the Central System on a hit or no hit basis only. This is to safeguard the right of access to this data, thus where there is no fingerprint or facial image match the personal data cannot be obtained.

For the purposes of the Dublin Regulation, new information is required to be updated in EURODAC relating to the Member State that becomes responsible for examining an asylum application following allocation of an applicant to another Member State. This will then make clear which Member State is responsible under the recast Dublin Regulation, if an applicant absconds or claims asylum in another Member State following an allocation procedure and a fingerprint hit.

- Biometric identifiers (Articles 2, 15, and 16): The current EURODAC Regulation allows for the comparison of fingerprint data only. In 2015, the European Agenda on Migration suggested the possibility to add other biometric identifiers to EURODAC in order to mitigate some of the challenges Member States were facing with damaged fingertips and non-compliance with the fingerprint process.[21] This proposal inserts a requirement for Member

[20] SWD(2015) 150 final

[21] Communication from The Commission to The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A European Agenda On Migration, COM(2015) 240 final, 13.5.2015, pp13-14.

States to take a facial image of the data-subject for transmission to the Central System and includes provisions to make a comparison of fingerprint and facial image data together and facial images separately under defined conditions. The insertion of facial images into the Central System now will prime the system for searches to be made with facial recognition software in the future.

Member States will continue to take the fingerprints of all ten fingers as plain and rolled impressions and this will now apply to individuals who are found illegally staying in a Member State because the same set of fingerprints will be needed for all three categories to be compared accurately.

- Comparison and transmission of all categories of all data (Articles 15 and 16): whereas under Regulation (EU) No. 603/2013, only two fingerprint categories were stored and data could only be searched against fingerprint data of applicants for international protection, the fingerprint and facial image data of all three categories of data will now be stored and compared against each other. This will allow the immigration authorities in a Member State to ascertain whether an illegally staying third-country national in a Member State has claimed asylum, or has entered the EU illegally at the external border. In the same vein it will allow a Member State to check whether someone apprehended crossing the external border irregularly was ever illegally staying in another Member State. Widening the scope of searches allows a pattern of irregular and secondary movements to be followed throughout the European Union, and can lead to establishing the identity of the individual concerned in the absence of valid identity documents.

- Lowering the age of taking fingerprints to 6 years old (Articles 10, 13 and 14): the age for taking fingerprints has always historically been 14 years of age. The study conducted by the Commission's Joint Research Centre, on *'Fingerprint Recognition for children*'[22] indicates that fingerprints taken from children age six and above can be used in automated matching scenarios such as EURODAC when sufficient care is taken to acquire good quality images.

Indeed many Member States take the fingerprints of children at a lower age than six for national purposes, such as issuing a passport or a biometric residence permit.

Many applicants for international protection and third-country nationals arriving irregularly to the European Union travel with families and in many cases very young children. Being able to identify these children with the help of fingerprints and facial images will help identify children in cases where they are separated from their families by allowing a Member State to follow up a line of inquiry where a fingerprint match indicates that they were present in another Member State. It would also strengthen the protection of unaccompanied minors who do not always formally seek international protection and who abscond from care institutions or child social services under which their care has been assigned. Under the current legal and technical framework their identity cannot be established. Thus the EURODAC system could be used to register children from third-countries where they are found undocumented within the EU to help keep track of them and prevent them from ending up in scenarios of exploitation.

- Data retention (Article 17): the data retention period of applicants for international protection remains the same at 10 years. This is to ensure that Member States can track secondary movements within the European Union following a grant of international protection status where the individual concerned is not authorised to reside in another Member State. Given that the recast Dublin Regulation will include in its scope beneficiaries

[22] (Report EUR 26193 EN; ISBN 978-92-79-33390-3)

of international protection, this data can now be used to transfer back refugees or persons granted subsidiary protection status to the Member State that granted them such protection.

Fingerprint data for illegally staying third-country nationals who do not claim asylum will be retained for five years. This is because EURODAC is no longer a database for asylum applicants only and retaining this data for longer is necessary to ensure that illegal immigration and secondary movements within and to the EU can be sufficiently monitored. This storage period is aligned with the maximum period for placing an entry ban on an individual for migration purposes as set out in Article 11 of the Returns Directive 2008/115/EC, the data retention period for storing information on a visa (Article 23 of the Visa Regulation), and the proposed data retention period for storing data in the Entry/Exit System (Article 31 of the EES).

- Advanced data erasure (Article 18): advanced data erasure remains the same for applicants for international protection and irregular third-country nationals or stateless persons who are granted citizenship. Data belonging to these individuals that is stored in the central system will be deleted in advance if citizenship of a Member State is obtained because they no longer fall within the scope of EURODAC.

Data will no longer be deleted in advance for illegally staying third-country nationals or stateless persons who were granted a residence document or left the territory of the European Union. It is necessary to retain this data in case at some point a residence document, which normally confers limited leave, is no longer valid and the individual overstays, or the illegally staying third-country national who had returned to a third country may attempt to re-enter the EU in an irregular manner again.

- Marking of data for illegally staying third-country nationals (Article 19 (4) and (5)): Currently under the EURODAC Regulation, the data of illegally staying third-country nationals who do not lodge an application for asylum within the European Union is erased in advance once a residence document is obtained. The proposal introduces changes to allow for this data to be marked instead of erased in advance, so that when a Member State conducts a search in EURODAC, which results in a marked hit from the Central system, it can ascertain immediately that the illegally staying third-country national has been given a residence document by another Member State. It may then be possible, under Article 6(2) of the Return Directive to pass back the individual to the Member State that issued the residence document.

Data for applicants for international protection is blocked for law enforcement purposes after three years; however, the data of illegally staying third-country nationals, who do not apply for international protection and who have been granted a temporary residence document, will not be blocked for law enforcement purposes. This is to ensure that where a residence document expires before the five-year data retention period lapses, the data is still searchable. Data belonging to asylum applicants will continue to be treated differently in this respect because asylum applicants are more likely to obtain a renewal of their residence permit as a beneficiary of international protection or a long-term residence permit.

-Sharing information obtained from EURODAC with third-countries (Article 38): sharing information with a third country, international organisation or private entity is strictly prohibited under the current Regulation. Extending the scope of EURODAC to assist a Member State to use EURODAC data for identifying and re-documenting an illegally staying third-country national for return and readmission purposes will necessarily entail sharing that data in some circumstances, with a third country - for the legitimate and sole purposes of return. Thus a specific provision to allowing sharing data with third countries for return purposes has been included, that sets out very strict conditions under which this data can be shared. It also strictly forbids the EURODAC database to be accessed by a third country,

which is not a party to the Dublin Regulation, or to allow a Member State to check data on behalf of a third country. By adding this provision on sharing data with third countries, EURODAC is aligned with other databases such as the VIS and the Entry/Exit System that also contain similar provisions for sharing information for return purposes.

- Access for law enforcement authorities and EUROPOL(Article 20 (3)): minor amendments have been made to the provisions for law enforcement access to make sure that all three categories of data stored in the Central System can be compared against when a law enforcement search is carried out and to allow in the future, a search based on a facial image.

-Allowing European Border and Coast Guards and EASO Member State experts to take fingerprints (Article 10(3) and 13 (7): the proposal permits, at the discretion of a Member State, the European Border [and Coast] Guard Agency and Member State's asylum experts that are deployed to a Member State under the auspices of EASO, to take and transmit fingerprints to EURODAC on behalf of a Member State. The proposal limits these functions to areas where both Agencies' mandates permit them do this (i.e. at the external border for those entering illegally and for asylum applicants).

- Statistics (Article 9): to allow for more transparency of EURODAC data, amendments have been made to the type of statistics that are published and the frequency of publication by eu-LISA. New provisions have been included to allow for statistical data obtained from EURODAC to be shared with the relevant Justice and Home Affairs Agencies for analysis and research purposes. Statistics produced by eu-LISA for these purposes should not report any names, individual date of births, or any personal data that would individually identify a data-subject. Amendments have also been introduced to allow the Commission to request ad-hoc statistics from eu-LISA on request.

- Architecture and operational management of the Central System (Article 4 and 5): changes have been made to the communication infrastructure to allow for the Central System to make use of the Eurodomain, which will bring significant economies of scale. The operational management of DubliNet as an existing separate communication infrastructure for the purposes of the Dublin Regulation has also been incorporated under the system architecture and will ensure that both its financial and operational management is transferred to eu-LISA, who currently is only responsible for its operational management via a separate Memorandum of Understanding with the Commission (DG HOME).

- Providing information on false hits (Article 26(6)): Member States will now be required to inform only eu-LISA of the fact that a false hit was received by the Central System and give eu-LISA information relating to that hit so that they can unlink the false hit records from the database. In the future eu-LISA will compile statistics on the number of reported false hits so that the Commission will no longer need to be informed directly of a false hit.

- Using real personal data for testing (Article 5(1)): When it has come to testing the EURODAC Central System, eu-LISA has been restricted to using 'dummy data' for the test environment and to test new technologies, which has failed to yield good test results because of the data used. The proposal allows for the use of real personal data when testing the Central System for diagnostics and repair, as well as the use of new technologies and techniques, subject to stringent conditions and on the basis that the data is anonymised for the testing purposes and cannot be used for individual identification.

↓ 603/2013 (adapted)

2016/0132 (COD)

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) 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 Data Protection Supervisor,

Acting in accordance with the ordinary legislative procedure,

Whereas:

↓ 603/2013 recital 1 (adapted)

(1) A number of substantive changes are to be made to ~~Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention~~[23] ~~and to Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention~~[24] ⌦ Regulation (EU) No 603/2013 of the European Parliament and of the Council[25] ⌫ . In the interests of clarity, ~~those~~ ⌦ that ⌫ Regulation~~s~~ should be recast.

23 ~~OJ L 316, 15.12.2000, p. 1.~~

24 ~~OJ L 62, 5.3.2002, p. 1.~~

25 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

↓ 603/2013 recital 2

(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.

↓ 603/2013 recital 3 (adapted)

(3) ~~The European Council of 4 November 2004 adopted The Hague Programme which set the objectives to be implemented in the area of freedom, security and justice in the period 2005-2010. The European Pact on Immigration and Asylum endorsed by the European Council of 15-16 October 2008 called for the completion of the establishment of a Common European Asylum System by creating a single procedure comprising common guarantees and a uniform status for refugees and for persons eligible for subsidiary protection.~~

↓ 603/2013 recital 4 (adapted)

(4) For the purposes of applying Regulation (EU) No […/…] ~~of the European Parliament and of the Council[26]~~ of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person[27], 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.

(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).

26 ~~Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person (OJ L 180, 29.6.2013, p. 31).~~

27 See page 31 of this Official Journal.

🡻 603/2013 recital 5 (adapted)
⇨ new

(5) ~~Fingerprints~~ ⇨ 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 fingerprint ⇨ and facial image ⇦ data.

🡻 603/2013 recital 6
⇨ new

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

⇩ new

(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.

🡻 603/2013 recital 7 (adapted)

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

⇩ new

(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"[28] 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)*".

[28] COM(2015) 240 final, 13.5.2015

(10) To assist Member States overcome challenges relating to non-compliance with the fingerprinting process, this Regulation also permits the comparison of a facial image without fingerprints as a last resort, 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. 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 where non-compliance based on reasons not relating to the conditions of the individual's fingertips are given. Where facial images are used in combination with fingerprint data, it allows for the reduction of fingerprints registered while enabling the same result in terms of accuracy of the identification.

(11) The return of third-country nationals 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[29], 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 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.

(12) National authorities in the Member States experience difficulties in identifying illegally staying third-country nationals 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 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, 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 staytng third-country national 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[30]. 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 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.

---

[29] 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.

[30] EU Action Plan on return, COM(2015) 453 final.

(14) The Commission's Communication on Stronger and Smarter Information Systems for Borders and Security[31] 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 Systems (SIS) and the Visa Information Systems (VIS), and examine if there is a need to revise the legal framework for law enforcement access to EURODAC.

↓ 603/2013 recital 8

(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 ~~of 13 June 2002 on combating terrorism~~[32] or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA ~~of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States~~[33]. 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).

↓ 603/2013 recital 9

(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.

↓ 603/2013 recital 10 (adapted)

(17) The Commission ~~outlines~~ ⌦ 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

---

[31] COM(2016) 205 final

[32] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3~~)~~).

[33] 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).

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.

↓ 603/2013 recital 11

(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 ~~of 6 April 2009 establishing the European Police Office (Europol)~~[34].

↓ 603/2013 recital 12

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

↓ 603/2013 recital 13
⇨ new

(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, ⇦ ~~A~~any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary ~~in a democratic society to protect a legitimate and proportionate~~ ⇨ to genuinely meet an objective of general ⇦ interest and proportionate to the legitimate objective it aims to achieve.

↓ 603/2013 recital 14

(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,

---

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

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.

↓ 603/2013 recital 15

(22) This Regulation also lays down the conditions under which requests for comparison of fingerprint data with Eurodac data for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences should be allowed and the necessary safeguards to ensure the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac. The strictness of those conditions reflects the fact that the Eurodac database registers fingerprint data of persons who are not presumed to have committed a terrorist offence or other serious criminal offence.

↓ 603/2013 recital 16 (adapted)

(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 ~~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~~[35] and Regulation (EU) No […/…]~~604/2013~~, ~~it is appropriate to extend the scope of~~ this Regulation ~~in order to include~~ ⌦ includes ⌫ applicants for subsidiary protection and persons eligible for subsidiary protection ⌦ in its scope ⌫ .

↓ 603/2013 recital 17
⇨ new

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

---

[35] 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).

⇩ new

(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 fingerprints and a facial image 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 is closely linked to the determination of the best interests of the child and eventually, the determination of a durable solution.

(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.

🡻 603/2013 recital 18 (adapted)
⇨ new

(27) It is necessary to lay down precise rules for the transmission of such fingerprint ⇨ and facial image ⇦ data to the Central System, the recording of such fingerprint ⇨ and facial image ⇦ data and of other relevant ⌦ personal ⌫ data in the Central System, their storage, their comparison with other fingerprint ⇨ and facial image ⇦ 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.

🡻 603/2013 recital 19 (adapted)
⇨ new

(28) Member States should ensure the transmission of fingerprint ⇨ and facial image ⇦ 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[36] (~~the "Agency"~~ ⌦ "eu-LISA" ⌫) of specific difficulties encountered with regard to the quality of data, in order to resolve them.

[36] 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).

↓ 603/2013 recital 20
⇨ new

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

⇩ new

(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 adopted by the Council on 20 July 2015[37], which sets out a best practice approach to taking fingerprints of irregular third-country nationals. 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 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.

↓ 603/2013 recital 21 (adapted)
⇨ new

(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 […/…]~~604/2013~~ ⇨ ; 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 where there is doubt that the result relates to the same person. ⇦

↓ 603/2013 recital 22 (adapted)
⇨ new

(32) Third-country nationals or stateless persons who have requested international protection in one Member State may ~~have the option of~~ ⇨ try to ⇦ request~~ing~~ international protection in another Member State for many years to come. Therefore, the maximum period during which fingerprint ⇨ and facial image ⇦ 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

[37] COM(2015) 150 final, 27.5.2015

period, a period of ten years should be considered a reasonable period for the storage of fingerprint ⇨ and facial image ⇦ data.

⇩ new

(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[38] and the right to protection of personal data, a period of five years should be considered a necessary period for the storage of fingerprint and facial data.

🡻 603/2013 recital 23
⇨ new

(34) The storage period should be shorter in certain special situations where there is no need to keep fingerprint ⇨ and facial ⇦ data ⇨ and all other personal data ⇦ for that length of time. Fingerprint ⇨ and facial image ⇦ data ⇨ and all other personal data belonging to a third-country national ⇦ should be erased immediately once third-country nationals or stateless persons obtain citizenship of a Member State.

🡻 603/2013 recital 24
⇨ new

(35) It is appropriate to store data relating to those data subjects whose fingerprints ⇨ and facial images ⇦ 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.

🡻 603/2013 recital 25 (adapted)

(36) ~~The Agency~~ ⌦ 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 ~~the Agency~~ ⌦ eu-LISA ⌫ took up its responsibilities on 1 December 2012. ~~The Agency should take up the tasks entrusted to it under this Regulation, and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly.~~ In addition, Europol should have observer status at the meetings of the Management Board of ~~the Agency~~ ⌦ 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

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

on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of ⊠ eu-LISA ⊠ ~~the Agency~~.

↓ 603/2013 recital 26

~~The Staff Regulations of Officials of the European Union (Staff Regulations of Officials) and the Conditions of Employment of Other Servants of the European Union ('Conditions of Employment'), laid down in Regulation (EEC, Euratom, ECSC) No 259/68 of the Council[39] (together referred to as the 'Staff Regulations') should apply to all staff working in the Agency on matters pertaining to this Regulation.~~

↓ 603/2013 recital 27 (adapted)

(37) It is necessary to lay down clearly the respective responsibilities of the Commission and ⊠ eu-LISA ⊠ ~~the Agency~~, in respect of the Central System and the Communication Infrastructure, and of the Member States, as regards data processing, data security, access to, and correction of~~,~~ recorded data.

↓ 603/2013 recital 28

(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.

↓ 603/2013 recital 29

(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.

---

[39] ~~OJ L 56, 4.3.1968, p. 1.~~

↓ 603/2013 recital 30

(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.

↓ 603/2013 recital 31

(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.

↓ 603/2013 recital 32

(42) In addition, access should be allowed only on condition that comparisons with the national fingerprint databases of the Member State and with the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA ~~of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime~~[40] did not lead to the establishment of the identity of the data subject. That condition requires the requesting Member State to conduct comparisons with the automated fingerprinting identification systems of all other Member States under Decision 2008/615/JHA which are technically available, unless that Member State can justify that there are reasonable grounds to believe that it would not lead to the establishment of the identity of the data subject. Such reasonable grounds exist in particular where the specific case does not present any operational or investigative link to a given Member State. That condition requires prior legal and technical implementation of Decision 2008/615/JHA by the requesting Member State in the area of fingerprint data, as it should not be permitted to conduct a Eurodac check for law enforcement purposes where those above steps have not been first taken.

[40] 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).

↓ 603/2013 recital 33

(43) Prior to searching Eurodac, designated authorities should also, provided that the conditions for a comparison are met, consult the Visa Information System under Council Decision 2008/633/JHA ~~of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences~~[41].

↓ 603/2013 recital 34

(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.

↓ 603/2013 recital 35

~~The best interests of the child should be a primary consideration for Member States when applying this Regulation. Where the requesting Member State establishes that Eurodac data pertain to a minor, these data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws applicable to minors and in accordance with the obligation to give primary consideration to the best interests of the child.~~

↓ 603/2013 recital 36

(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.

↓ 603/2013 recital 37 (adapted)
⇨ new

(46) Since the objective of this Regulation, namely the creation of a system for the comparison of fingerprint ⇨ and facial image ⇦ 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

[41] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

↓ 603/2013 recital 38 (adapted)
⇨ new

(47) [Directive [2016/…/…] 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~~[42]] 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 ~~investigation~~ ⇨ prosecution ⇦ of terrorist offences or of other serious criminal offences ⇨ including the safeguarding against and the prevention of threats to public security ⇦ .

↓ 603/2013 recital 39 (adapted)
⇨ new

(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 ⌫ ~~T~~the processing of personal data by ~~the~~ ⌦ competent ⌫ authorities of the Member States for the purposes of the prevention, ⌦ investigation, ⌫ detection or ~~investigation~~ ⇨ prosecution ⇦ of terrorist offences or of other serious criminal offences pursuant to this Regulation ~~should be subject to a standard of protection of personal data under their national law which complies with Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters~~[43].

↓ 603/2013 recital 40 (adapted)
⇨ new

(49) The ~~principles~~ ⇨ rules ⇦ set out in Regulation ~~Directive~~ [2016/…/..] ~~95/46/EC~~ regarding the protection of the rights and freedoms of individuals, notably their right to ⌦ the protection of personal data concerning them ⌫ ~~privacy~~, 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 ⇦ ~~supplemented or clarified~~, in particular as far as certain sectors are concerned.

---

42 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).

43 ~~OJ L 350, 30.12.2008, p. 60.~~

↓ 603/2013 recital 41
⇨ new

(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 fingerprints were taken as well as the date on which the Member State(s) transmitted the data to Eurodac; the operator user ID; and any information relating to any transfer of the data subject under [Regulation (EU) No 604/2013]. That prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which [Regulation (EU) No 604/2013] applies [⇨ in accordance with Regulation (EU) No […/2016]respectively with the national rules adopted pursuant to Directive [2016/…/EU] ⇦], in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

⇩ new

(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 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 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 must be in accordance with the provisions of Chapter V of Regulation (EU) No. […2016].

↓ 603/2013 recital 42

(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.

↓ 603/2013 recital 43

(53) 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~~[44], 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].

↓ 603/2013 recital 44 (adapted)
⇨ new

(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) […/…] ~~No 604/2013~~, and of the use to which law enforcement authorities may put his or her data.

↓ 603/2013 recital 45

(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.

⇩ new

(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 […]

↓ 603/2013 recital 46

(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.

↓ 603/2013 recital 47 (adapted)

(58) It is appropriate to monitor and evaluate the performance of Eurodac at regular intervals, including in terms of whether law enforcement access has led to indirect

---

[44] 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).

discrimination against applicants for international protection, as raised in the Commission's evaluation of the compliance of this Regulation with the Charter of Fundamental Rights of the European Union ('the Charter'). ~~The Agency~~ ⌦ eu-LISA ⌫ should submit an annual report on the activities of the Central System to the European Parliament and to the Council.

↓ 603/2013 recital 48
⇨ new

(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.

↓ 603/2013 recital 49

(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.

↓ 603/2013 recital 50

(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.

↓ 603/2013 recital 51

(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.

↓ 603/2013 recital 52 (adapted)

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

↓ 603/2013 recital 53 (adapted)

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

~~to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.~~

⇩ new

(63) [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, those Member States have notified their wish to take part in the adoption and application of this Regulation] OR

(64) [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, those Member States are not taking part in the adoption of this Regulation and are not bound by it or subject to its application.] OR

(65) [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, the United Kingdom is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(66) 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, Ireland has notified (, by letter of ...,) its wish to take part in the adoption and application of this Regulation.] OR

(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 ...,) 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.]

🡻 603/2013 recital 54 (adapted)

(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 […/…] ~~604/2013~~,

↓ 603/2013 (adapted)

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 […/…] ~~604/2013~~ for examining an application for international protection lodged in a Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No […/…] ~~604/2013~~ under the conditions set out in this Regulation~~.~~;

⇩ new

(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 for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation.

↓ 603/2013 (adapted)
⇨ new

~~2.~~ (c) ~~This Regulation also~~ lay~~s~~ down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint ⇨ and facial image ⇦ 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 ⇦ .

~~3~~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, fingerprint data and other personal data may be processed in Eurodac only for the purposes set out in this Regulation and [Article 34(1) of Regulation (EU) No 604/2013].

Article 2

Obligation to take fingerprints and a facial image

1. Member States are obliged to take the fingerprints and facial image 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 fingerprints and a facial image and inform them as such in accordance with Article 30 of this Regulation.

2. Taking fingerprints and facial images 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 facial images. The minor shall be informed in an age-appropriate manner using leaflets and/or infographics and/or demonstrations specifically designed to explain the fingerprinting and facial image procedure to minors and they shall be accompanied by a responsible adult, guardian or representative at the time their fingerprints and facial image 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 may introduce administrative sanctions, in accordance with their national law, for non-compliance with the fingerprinting process and capturing a facial image in accordance with paragraph 1 of this Article. These sanctions shall be effective, proportionate and dissuasive. 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 identity.

4. Without prejudice to paragraph 3 of this Article, where enrolment of the fingerprints or facial image is not possible from third-country nationals 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 fingerprints or a facial image. A Member State may attempt to re-take the fingerprints or facial image 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 fingerprints or a facial image 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.

↓ 603/2013
⇨ new

5. The procedure for taking fingerprints ⇨ and a facial image ⇦ 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 ~~2~~ 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 ~~9~~ 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 ~~14~~ 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 ~~17~~ 14(1), the Member State which transmits the personal data to the Central System and receives the results of the comparison;

⇩ new

(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 European Union;

⇩ new

(d) 'illegal stay' means the presence on the territory of a Member State, of a third-country national who does not fulfill, 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;

🡻 603/2013 (adapted)
⇨ new

(~~c~~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;

(~~d~~f)'hit' means the existence of a match or matches established by the Central System by comparison between fingerprint data recorded in the computerised central database and those transmitted by a Member State with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article ~~25~~ 26(4);

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

(~~f~~h)~~'Agency'~~ ⌦ '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;

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

(~~h~~j)'Eurodac data' means all data stored in the Central System in accordance with Article ~~11~~ 12, ~~and~~ Article ~~14~~ 13(2) ⇨ and Article 14(2) ⇦ ;

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

(~~j~~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;

(~~k~~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;

(~~l~~n)'fingerprint data' means the data relating to ⇨ plain and rolled impressions of the ⇦ fingerprints of all ⇨ ten fingers, where present ⇦ ~~or at least the index fingers, and if those are missing, the prints of all other fingers of a person~~, or a latent fingerprint~~.~~;

⇩ new

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

🡻 603/2013 (adapted)
⇨ new

2. The terms defined in Article [..]~~2~~ of Directive [2016/…/EU[~~95/46/EC~~ shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of the Member States for the purposes laid down in Article 1(1)(a) of this Regulation.

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

4. The terms defined in Article […] ~~2~~ of Directive [2016/…/EU]~~Framework Decision 2008/977/JHA~~ 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~~(2)~~(1)(c) of this Regulation.

Article ~~3~~ 4

System architecture and basic principles

1. Eurodac shall consist of:

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

(i) a Central Unit,

(ii) a Business Continuity Plan and System;

(b) a communication infrastructure between the Central System and Member States that provides ~~an encrypted virtual network dedicated to~~ ⇨ a secure and encrypted communication channel for ⇦ Eurodac data ("Communication Infrastructure").

⇩ new

2. The EURODAC Communication Infrastructure will be using the existing 'Secure Trans European Services for Telematics between Administrations' (TESTA) network. A separate virtual private network dedicated to the EURODAC shall be established on the existing TESTA private virtual network to ensure the logical separation of EURODAC data from other data.

🡻 603/2013

~~2~~3. Each Member State shall have a single National Access Point.

~~3~~4. Data on persons covered by Articles ~~9~~ 10(1), ~~14~~ 13(1) and ~~17~~ 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.

~~4~~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.

🡻 603/2013 (adapted)

Article ~~4~~ 5

Operational management

1. ~~The Agency~~ ⌦ 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.

~~The Agency~~ ⌦ 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.

⇩ new

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.

↓ 603/2013 (adapted)

~~2~~3. ~~The Agency~~ ⌦ 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.

~~3~~4. The Commission shall be responsible for all tasks relating to the Communication Infrastructure other than those referred to in paragraph ~~2~~ 3, in particular:

(a) the implementation of the budget;

(b) acquisition and renewal;

(c) contractual matters.

⇩ new

5. 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.

↓ 603/2013 (adapted)
⇨ new

~~4~~6. Without prejudice to Article 17 of the Staff Regulations, ~~the Agency~~ ⌦ 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 ~~5~~ 6

Member States' designated authorities for law enforcement purposes

1. For the purposes laid down in Article 1~~(2)~~(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. Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security.

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

3. Each Member State shall keep a list of the operating units within the designated authorities that are authorised to request comparisons with Eurodac data through the National Access Point.

Article ~~6~~ 7

Member States' verifying authorities for law enforcement purposes

1. For the purposes laid down in Article 1~~(2)~~(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 ~~5~~ 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 fingerprints with Eurodac data are fulfilled.

Only duly empowered staff of the verifying authority shall be authorised to receive and transmit a request for access to Eurodac in accordance with Article ~~19~~ 20.

Only the verifying authority shall be authorised to forward requests for comparison of fingerprints ⇨ and facial images ⇦ to the National Access Point.

Article ~~7~~ 8

Europol

1. For the purposes laid down in Article 1~~(2)~~(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 fingerprints ⇨ and facial images ⇦ with Eurodac data are fulfilled. Europol shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint ⇨ and facial image ⇦ data to the Central System.

2. For the purposes laid down in Article 1~~(2)~~ (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 ~~8~~ 9

Statistics

1. ~~The Agency~~ ⌦ eu-LISA ⌫ shall draw up statistics on the work of the Central System every ⇨ month ⇦ ~~quarter~~, indicating in particular:

(a) the number of data sets transmitted on persons referred to in Articles ~~9~~ 10(1), ~~14~~ 13(1) and ~~17~~ 14(1);

(b) the number of hits for ~~applicants for international protection~~ ⌦ 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 ~~14~~ 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 ~~17~~ 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 fingerprint data which the Central System had to request more than once from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;

(f) the number of data sets marked, unmarked, blocked and unblocked in accordance with Article ~~18~~ 19(1) and ~~(3)~~ ⇨ 17(2), (3) and (4) ⇦ ;

(g) the number of hits for persons referred to in Article ~~18~~ 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 ~~20~~ 21(1);

(i) the number of requests and hits referred to in Article ~~21~~ 22(1)~~.~~;

⇩ new

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

(h) the number of hits received from the Central System as referred to in Article 26(6).

🡻 603/2013 (adapted)
⇨ new

2. ⇨ The monthly statistical data for persons referred to in paragraph1(a) to (h) 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 (h) ⇦ shall be ⇨ published and made public by eu-LISA ⇦ ~~established in the form of a compilation of the quarterly statistics for that year, including an indication of the number of persons for whom hits have been~~

~~recorded under paragraph 1(b), (c) and (d)~~. The statistics shall contain a breakdown of data for each Member State. ~~The results shall be made public.~~

⇩ new

3. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects for research and analysis purposes without allowing for individual identification as well as the possibility to produce regular statistics pursuant to paragraph 1. These statistics shall be shared with other Justice and Home Affairs Agencies if they are relevant for the implementation of their tasks.

🡻 603/2013 (adapted)
⇨ new

CHAPTER II

APPLICANTS FOR INTERNATIONAL PROTECTION

Article ~~9~~ 10

Collection~~,~~ ⌦ and ⌫ transmission ~~and comparison~~ of fingerprints ⌦ and facial image data ⌫

1. Each Member State shall promptly take the fingerprints of all fingers ⇨ and capture a facial image ⇦ of every applicant for international protection of at least ~~14~~ ⇨ 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 ~~604/2013~~, transmit them together with the data referred to in Article ~~11~~ 12~~(b) to (g)~~ ⇨ (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 fingerprints to the Central System. Where the condition of the fingertips does not allow the taking of the fingerprints of a quality ensuring appropriate comparison under Article ~~25~~ 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 fingerprints ⇨ and facial image ⇦ of an applicant for international protection on account of measures taken to ensure his or her health or the protection of public health, Member States shall take and send such fingerprints ⇨ and facial image ⇦ as soon as possible and no later than 48 hours after those health grounds no longer prevail.

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

~~3. Fingerprint data within the meaning of Article 11(a) transmitted by any Member State, with the exception of those transmitted in accordance with Article 10(b), shall be compared~~

~~automatically with the fingerprint data transmitted by other Member States and already stored in the Central System.~~

~~4. The Central System shall ensure, at the request of a Member State that the comparison referred to in paragraph 3 covers the fingerprint data previously transmitted by that Member State, in addition to the data from other Member States.~~

~~5. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin. Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 11(a) to (k) along with, where appropriate, the mark referred to in Article 18(1).~~

⇩ new

3. Fingerprint 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].

🡻 603/2013 (adapted)
⇨ new

Article ~~10~~ 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 ~~12~~ 17 (1) for the purpose of transmission under Articles ~~9(5)~~ ⇨ 15 and 16 ⇦ :

(a) when an applicant for international protection or another person as referred to in ⇨ Article 21(1) ⇦ ⇨ (b), (c), ⇦ (d) ⇨ or (e) ⇦ of Regulation (EU) No […/…] ~~604/2013~~ arrives in the Member State responsible following a transfer pursuant to ~~a decision acceding to~~ a take back ~~request~~ ⇨ notification ⇦ as referred to in Article ⇨ 26 ⇦ thereof, the Member State responsible shall update its data set recorded in conformity with Article ~~11~~ 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 […/…] ~~604/2013~~, the Member State responsible shall send a data set recorded in conformity with Article ~~11~~ 12 of this Regulation relating to the person concerned and shall include his or her date of arrival;

⇩ new (adapted)

(c) when an applicant for international protection arrives in the Member State of allocation pursuant to Article 34 of Regulation (EU) No. […/…] ~~604/2013~~, 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.

🡻 603/2013 (adapted)
⇨ new

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

(d) as soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with Article ~~11~~ 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 ~~as provided for in Article 19(3) of Regulation (EU) No 604/2013~~, it shall update its data set recorded in conformity with Article ~~11~~ 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 […/…] ~~604/2013~~ shall update its data set recorded in conformity with Article ~~11~~ 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 ~~11~~ 12

Recording of data

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

(a) fingerprint data;

⇩ new

(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(ies);

(e) place and date of birth;

↓ 603/2013

(~~b~~f) Member State of origin, place and date of the application for international protection; in the cases referred to in Article ~~10~~ 11(b), the date of application shall be the one entered by the Member State who transferred the applicant;

(~~c~~g) sex;

⇩ new

(h) type and number of identity or travel document; three letter code of the issuing country and validity;

↓ 603/2013

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

⇩ new (adapted)

(j) unique application number of the application for international protection pursuant to Article 22(2) of Regulation (EU) No. […/…]~~604/2013~~;

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

↓ 603/2013 (adapted)
⇨ new

(~~e~~l) date on which the fingerprints ⇨ and/or facial image ⇦ were taken;

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

(~~g~~n) operator user ID;

(~~h~~o) where applicable in accordance with Article ~~10~~ 11(a) ~~or (b)~~, the date of the arrival of the person concerned after a successful transfer;

⌦ (p) where applicable in accordance with Article ~~10~~ 11(b), the date of the arrival of the person concerned after a successful transfer; ⌫

⇩ new

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

↓ 603/2013 (adapted)
⇨ new

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

(~~j~~r) where applicable in accordance with Article ~~10~~ 11(d), the date when the person concerned left or was removed from the territory of the Member States;

(~~k~~s) where applicable in accordance with Article ~~10~~ 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 ~~14~~ 13

Collection and transmission of fingerprint data ⌦ and facial image data ⌫

1. Each Member State shall promptly take the fingerprints of all fingers ⇨ and capture a facial image ⇦ of every third-country national or stateless person of at least ~~14~~ ⇨ 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.

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;

⇩ new

(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(ies);

(e) place and date of birth

↓ 603/2013

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

(~~e~~g) sex;

⇩ new

(h) type and number of identity or travel document; three letter code of the issuing country and validity;

🡻 603/2013
⇨ new

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

(~~e~~j) date on which the fingerprints ⇨ and/or facial image ⇦ were taken;

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

(~~g~~l) operator user ID~~.~~;

⇩ new

(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.

🡻 603/2013
⇨ new

3. By way of derogation from paragraph 2, the data specified in paragraph 2 relating to persons apprehended as described in paragraph 1 who remain physically on the territory of the Member States but are kept in custody, confinement or detention upon their apprehension for a period exceeding 72 hours shall be transmitted before their release from custody, confinement or detention.

4. Non-compliance with the 72-hour time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article ~~25~~ 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 fingerprints ⇨ and facial image ⇦ of the apprehended person on account of measures taken to ensure his or her health or the protection of public health, the Member State concerned shall take and send such fingerprints ⇨ and facial image ⇦ 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.

⇩ new

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. Fingerprint 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].

🡻 603/2013 (adapted)

~~*Article 15*~~

~~**Recording of data**~~

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

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

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

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

~~*Article 16*~~

~~**Storage of data**~~

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

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

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

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

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

3. The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data for the reason specified in paragraph 2(a) or (b) of this Article by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).

4. The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data for the reason specified in paragraph 2(c) of this Article by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or 14(1).

CHAPTER IV

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

Article ~~17~~ 14

Comparison ⌦ Collection and transmission ⌫ of fingerprint ⌦ and facial image ⌫ data

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

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

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

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

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

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

⇩ new

1. Each Member State shall promptly take the fingerprints of all fingers and capture a facial image of every third-country national or stateless person of at least six years of age who is found illegally staying within its territory.

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(ies);

(e) place and date of birth

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

(g) sex;

(h) type and number of identity or travel document; three letter code of the issuing country and validity;

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

(j) date on which the fingerprints and/or facial image 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

---

🡻 603/2013 (adapted)
⇨ new

3. The fingerprint data of a third-country national or a stateless person as referred to in paragraph 1 shall be transmitted to the Central System ~~solely for the purpose of comparison~~ ⇨ and compared ⇦ with the fingerprint data of ~~applicants for international protection~~ ⌦ persons fingerprinted for the purposes of Article ~~9~~ 10(1), ~~14~~ 13(1) and ~~17~~ 14(1) ⌫ transmitted by other Member States and already recorded in the Central System.

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

⇩ new

4. Non-compliance with the 72-hour time-limit referred to in paragraph 3 of this Article shall not relieve Member States of the obligation to take and transmit the fingerprints to the Central

System. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 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 fingerprints and facial image of the apprehended person on account of measures taken to ensure his or her health or the protection of public health, the Member State concerned shall take and send such fingerprints and facial image 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 Article 13(1) of this Regulation 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 of this Article relating to the person concerned by adding the date of his or her removal or when he or she left the territory.

↓ 603/2013 (adapted)
⇨ new

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

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

CHAPTER V

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

Article 15

⌦ Comparison of fingerprint and facial image data ⌫

~~3~~1. Fingerprint ⇨ and facial image ⇦ data ~~within the meaning of Article 11(a)~~ transmitted by any Member State, with the exception of those transmitted in accordance with Article ~~10~~ 11(b) ⇨ and (c) ⇦ , shall be compared automatically with the fingerprint data transmitted by other Member States and already stored in the Central System ⌦ in accordance with Article ~~9~~ 10(1), ~~14~~ 13(1) and ~~17~~ 14(1) ⌫ .

~~4~~2. The Central System shall ensure, at the request of a Member State, that the comparison referred to in paragraph ~~3~~ 1 ⌦ of this Article ⌫ covers the fingerprint ⇨ and facial image ⇦ data previously transmitted by that Member State, in addition to the ⌦ fingerprint ⌫ ⇨ and facial image ⇦ data from other Member States.

~~5~~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 ~~11(a) to (k)~~ ⇨ 12, 13(2) and 14(2) ⇦ along with, where appropriate, the mark referred to in Article ~~18~~ 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. ⇦

⇩ new

4. Where evidence of 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.

⇩ new

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 or where a person referred to in Article 10(1), 13(1) and 14(1) refuses to comply with the fingerprinting process, a Member State may carry out a comparison of facial image data as a last resort.

(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(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 17(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 evidence of 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.

↓ 603/2013 (adapted)

CHAPTER ~~V~~ VI

~~*BENEFICIARIES OF INTERNATIONAL PROTECTION*~~ ⌦ DATA STORAGE, ADVANCED DATA ERASURE AND MARKING OF DATA ⌫

Article ~~12~~ 17

Data storage

1. ⌦ For the purposes laid down in Article 10(1), ⌫ ~~E~~each set of data ⌦ relating to an applicant for international protection ⌫ , as referred to in Article ~~11~~ 12, shall be stored in the Central System for ten years from the date on which the fingerprints were taken.

⇩ new

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 fingerprints 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 fingerprints were taken.

↓ 603/2013 (adapted)
⇨ new

~~2~~4. Upon expiry of the ~~period~~ ⌦ 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 ~~13~~ 18

~~Advance~~ ⌦ 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 ~~12~~17(1) ⇨ , (2) or (3) ⇦ shall be erased from the Central System in accordance with Article ~~27~~ 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 ~~9~~ 10(1)~~, or 14~~ 13(1) ⇨ or 14(1) ⇦ .

Article ~~18~~ 19

Marking of data

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 ~~11~~ 12 shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by ⌦ eu-LISA ⌫ ~~the Agency~~. That mark shall be stored in the Central System in accordance with Article ~~12~~ 17(1) for the purpose of transmission under Article ~~9(5)~~ ⇨ 15 ⇦ . 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 ~~9~~ 10(1)~~, or 14~~ 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~~(2)~~(1)(c) for a period of three years after the date on which the data subject was granted international protection.

Where there is a hit, the Central System shall transmit the data referred to in Article ~~11~~ 12~~(a) to (k)~~ ⇨ (b) to (s) ⇦ for all the data sets corresponding to the hit. The Central System shall not transmit the mark referred to in paragraph 1 of this Article. Upon the expiry of the period of three years, the Central System shall automatically block such data from being transmitted in the event of a request for comparison for the purposes laid down in Article 1~~(2)~~ (1)(c), whilst leaving those data available for comparison for the purposes laid down in Article 1(1)(a) until the point of their erasure. Blocked data shall not be transmitted, and the Central System shall return a negative result to the requesting Member State in the event of a hit.

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

⇩ new

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).

↓ 603/2013 (adapted)
⇨ new

CHAPTER ~~VI~~ VII

PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES

Article ~~19~~ 20

Procedure for comparison of fingerprint data with Eurodac data

1. For the purposes laid down in Article 1~~(2)~~(1)(c), the designated authorities referred to in Articles ~~5~~ 6(1) and ~~7~~ 8(2) may submit a reasoned electronic request as provided for in Article ~~20~~ 21(1) together with the reference number used by them, to the verifying authority for the transmission for comparison of fingerprint ⇨ and facial image ⇦ data to the Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether all the conditions for requesting a comparison referred to in Articles ~~20~~ 21 or ~~21~~ 22, as appropriate, are fulfilled.

2. Where all the conditions for requesting a comparison referred to in Articles ~~20~~ 21 or ~~21~~ 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 ~~9(3) and (5)~~ ⇨ 15 and 16 ⇦ for the purpose of comparison with the ⌦ fingerprint ⌫ ⇨ and facial image ⇦ data transmitted to the Central System pursuant to Articles ~~9~~ 10(1), ~~and~~ ~~14~~ 13~~(2)~~ ⇨ (1) and 14(1) ⇦ .

⇩ new

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).

↓ 603/2013 (adapted)
⇨ new

~~3~~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 fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions for requesting a comparison referred to in Article ~~20~~ 21 or Article ~~21~~ 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.

~~4~~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 ~~20~~ 21

Conditions for access to Eurodac by designated authorities

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

– national fingerprint databases;

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

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

and where the following cumulative conditions are met:

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

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

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

2. Requests for comparison with Eurodac data shall be limited to searching with fingerprint ⇨ or facial image ⇦ data.

Article ~~21~~ 22

Conditions for access to Eurodac by Europol

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

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

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

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

2. Requests for comparison with Eurodac data shall be limited to comparisons of fingerprint ⇨ and facial image ⇦ data.

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

Article ~~22~~ 23

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

1. Without prejudice to Article ~~26~~ 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~~(2)~~(1)(c), fingerprints shall be digitally processed by the Member States and transmitted in the data format ~~referred to~~ ⌦ as set out ⌫ in ⇨ the agreed Interface Control Document ⇦ ~~Annex I~~, in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.

CHAPTER ~~VII~~ VIII

DATA PROCESSING, DATA PROTECTION AND LIABILITY

Article ~~23~~ 24

Responsibility for data processing

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

(a) fingerprints ⇨ and facial images ⇦ are taken lawfully;

(b) fingerprint data and the other data referred to in Article ~~11~~ 12, Article ~~14~~ 13(2) and Article ~~17~~ 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 ⌫ ~~the Agency~~, data in the Central System are lawfully recorded, stored, corrected and erased;

(e) the results of fingerprint ⇨ and facial image ⇦ data comparisons transmitted by the Central System are lawfully processed.

2. In accordance with Article ~~34~~ 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.

3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article ~~25~~ 26(4).

4. ~~The Agency~~ ⌦ eu-LISA ⌫ shall ensure that the Central System is operated in accordance with the provisions of this Regulation. In particular, ~~the Agency~~ ⌦ 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 ~~34~~ 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.

~~The Agency~~ ⌦ 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 ~~24~~ 25

Transmission

1. Fingerprints shall be digitally processed and transmitted in the data format ~~referred to~~ ⌦ as set out ⌫ in ⇨ the agreed Interface Control Document ⇦ ~~Annex I~~. As far as necessary for the efficient operation of the Central System, ~~the Agency~~ ⌦ eu-LISA ⌫ shall establish the technical requirements for transmission of the data format by Member States to the Central System and vice versa. ~~The Agency~~ ⌦ eu-LISA ⌫ shall ensure that the fingerprint data ⇨ and facial images ⇦ 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 ~~11~~ 12, Article ~~14~~ 13(2) and Article ~~17~~ 14(2) electronically. The data referred to in Article ~~11~~ 12, ~~and~~ Article ~~14~~ 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, ~~the Agency~~ ⌦ 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 ~~11(d)~~ 12(i), ~~14(2)(d)~~ 13(2)(i), ~~17~~ 14~~(1)~~ ⇨ (2)(i) ⇦ and ~~19~~ 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 ~~9~~ 10(1), ~~14~~ 13(1) or ~~17~~ 14(1).

4. The reference number shall begin with the identification letter or letters by which~~, in accordance with the norm referred to in Annex I,~~ the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person or request. "1" refers to data relating to persons referred to in Article ~~9~~ 10(1), "2" to persons referred to in Article ~~14~~ 13(1), "3" to persons referred to in Article ~~17~~

14(1), "4" to requests referred to in Article ~~20~~ 21, "5" to requests referred to in Article ~~21~~ 22 and "9" to requests referred to in Article ~~29~~ 30.

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

Article ~~25~~ 26

Carrying out comparisons and transmitting results

1. Member States shall ensure the transmission of fingerprint data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint ⇨ 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, ~~the Agency~~ ⌦ eu-LISA ⌫ shall define the appropriate quality of transmitted fingerprint data. The Central System shall, as soon as possible, check the quality of the fingerprint ⇨ and facial image ⇦ data transmitted. If fingerprint ⇨ or facial image ⇦ 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 fingerprint ⇨ or facial image ⇦ data of the appropriate quality using the same reference number as the previous set of fingerprint ⇨ or facial image ⇦ data.

2. The Central System shall carry out comparisons in the order of arrival of requests. Each request shall be dealt with within 24 hours. A Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where such time-limits cannot be respected owing to circumstances which are outside the ~~Agency's~~ ⌦ 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, ~~the Agency~~ ⌦ 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, ~~the Agency~~ ⌦ 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. 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~~, pursuant to Article 34 of Regulation (EU) No 604/2013~~.

⇩ new

5. The result of the comparison of facial image data carried out pursuant to 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.

↓ 603/2013 (adapted) ⇨ new

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

~~5~~6. Where final identification in accordance with paragraph 4 reveals that the result of the comparison received from the Central System does not correspond to the fingerprint ⇨ or facial image ⇦ data sent for comparison, Member States shall immediately erase the result of the comparison and communicate this fact as soon as possible and no later than after three working days ~~to the Commission and~~ to ⌦ eu-LISA ⌫ ~~the Agency~~ ⇨ 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 ~~26~~ 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, ~~the Agency~~ ⌦ eu-LISA ⌫ shall establish the technical procedures necessary for the use of the Communication Infrastructure.

Article ~~27~~ 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 ~~9(5)~~ ⇨ 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 ~~the Agency~~ ⌦ eu-LISA ⌫ a list of those units and any amendments thereto. ~~The Agency~~ ⌦ eu-LISA ⌫ shall publish the consolidated list in the *Official Journal of the European Union*. Where there are amendments thereto, ~~the Agency~~ ⌦ 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 ⇦ ~~12(2) or 16(1)~~.

4. If a Member State or ~~the Agency~~ ⌦ 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], ⇦ 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 Agency~~, the Commission and the Member State of origin as soon as possible. The Member State of origin shall check the data concerned and, if necessary, amend or erase them without delay.

5. ~~The Agency~~ ⌦ 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 […/…]~~604/2013~~ applies.

Article ~~28~~ 29

Keeping of records

1. ~~The Agency~~ ⌦ 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 ⇦ ~~12(1) and in Article 16(1)~~ has expired, unless they are required for monitoring procedures which have already begun.

3. For the purposes laid down in Article 1(1)(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 ~~29~~ 30

Rights ⌦ of information ⌫ of the data subject

1. A person covered by Article ~~9~~ 10(1), Article ~~14~~ 13(1) or Article ~~17~~ 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 of the controller within the meaning of Article ~~2(d)~~ of Directive [../../EU]~~95/46/EC~~ 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, including a description of the aims of Regulation (EU) No […/…] ~~604/2013~~, in accordance with ⇨ Article 6 ⇦ thereof and an explanation in intelligible form~~, using clear and plain language,~~ of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;

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

(d) in relation to a person covered by Article ~~9~~ 10(1) or ~~14~~ 13(1) ⇨ or 14(1) ⇦ , the obligation to have his or her fingerprints taken;

⇩ new

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

↓ 603/2013 (adapted)
⇨ new

(~~e~~f) ⌦ the existence of ⌫ the right ⇨ to request from the controller ⇦ ~~of~~ access to data relating to him or her, and the right to request that inaccurate data relating to him or her be ~~corrected~~ ⌦ rectified ⌫ ⇨ and the completion of incomplete personal data ⇦ or that unlawfully processed ⌦ personal ⌫ data ~~relating to~~ ⌦ 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 ~~national~~ supervisory authorities referred to in Article ~~30~~ 32(1)~~.~~;

⇩ new

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

↓ 603/2013 (adapted)
⇨ new

2. In relation to a person covered by Article ~~9~~ 10(1) or ~~14~~ 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 fingerprints are taken.

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

Where a person covered by Article ~~9~~ 10(1), Article ~~14~~ 13(1) and Article ~~17~~ 14(1) is a minor, Member States shall provide the information in an age-appropriate manner.

3. A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in ⇨ Article 6(2) ⇦of Regulation (EU) No […/…] ~~604/2013~~ shall be drawn up in accordance with the procedure referred to in Article 44(2) of that Regulation.

The leaflet shall be clear and simple, drafted ⇨ in a 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 ~~assistance~~ ⇨ 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 ⌫

~~4~~1. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, ~~in each Member State any data subject may, in accordance with the laws, regulations and procedures of that State, exercise the rights provided for in Article 12 of Directive 95/46/EC~~ ⇨ the data subject's rights of access, rectification and erasure shall be exercised in accordance ,with Chapter III of Regulation (EU) No. […/2016] and applied as set out in this Article ⇦ .

~~Without prejudice to the obligation to provide other information in accordance with Article 12(a) of Directive 95/46/EC,~~ ⌦ 2. The right of access of ⌫ the data subject ⌦ in each Member State ⌫ shall ~~have~~ ⌦ 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.

~~5. For the purposes laid down in Article 1(1), in each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be carried out without excessive delay by the Member State which transmitted the data, in accordance with its laws, regulations and procedures.~~

~~6~~2. ~~For the purposes laid down in Article 1(1),~~ ~~i~~If the rights of ~~correction~~ ⌦ 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.

~~7~~3. ~~For the purposes laid down in Article 1(1),~~ ~~i~~If it emerges that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall ~~correct~~ ⌦ rectify ⌫ or erase the data in accordance with Article ~~27~~ 28(3). That Member State shall confirm in writing to the data subject ~~without excessive delay~~ that it has taken action to correct ⌦ , rectify, ⌫ ⇨ complete, ⇦ ~~or~~ erase ⇨ or restrict the processing of ⇦ ⌦ personal ⌫ data relating to him or her.

~~8~~4. ~~For the purposes laid down in Article 1(1),~~ ~~i~~If the Member State which transmitted the data does not agree that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject ~~without excessive delay~~ why it is not prepared to correct or erase the data.

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

~~9~~5. Any request under paragraphs ~~4~~ 1 and ~~5~~ 2 ⌦ of this Article for access, rectification or erasure ⌫ shall contain all the necessary particulars to identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the ⌦ data subject's ⌫ rights referred to in paragraphs ~~4~~ 1 and ~~5~~ 2 and shall be erased immediately afterwards.

~~10~~6. The competent authorities of the Member States shall cooperate actively to enforce promptly the ⌦ data subject's ⌫ rights ~~laid down in paragraphs 5, 6 and 7~~ ⌦ for rectification and erasure ⌫ .

~~11~~7. Whenever a person requests ⌦ access to ⌫ data relating to him or her ~~in accordance with paragraph 4~~, the competent authority shall keep a record in the form of a written document that such a request was made and how it was addressed, and shall make that document available to the national supervisory authorities without delay.

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

~~13~~8. ~~For the purposes laid down in Article 1(1) of this Regulation,~~ ~~t~~The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall ~~assist and~~, where requested, ~~advise him or her in exercising~~ ⌦ provide information to the data subject concerning the exercise of ⌫ his or her right to ⇨ request from the data controller access, ⇦ ~~correct~~ ⌦ rectification, ⌫ ⇨ completion, ⇦ ~~or erase~~ ⌦ erasure ⌫ ⇨ or restriction of the processing of ⇦ ⌦ personal ⌫ data ⌦ concerning him or her ⌫ . ~~Both national~~ ⌦ The ⌫ supervisory authorities shall cooperate ~~to this end~~ ⇨ in accordance with Chapter VII of Regulation (EU) […/2016] ⇦ . ~~Requests for such assistance may be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data.~~

~~14. In each Member State any person may, in accordance with the laws, regulations and procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he or she is refused the right of access provided for in paragraph 4.~~

~~15. Any person may, in accordance with the laws, regulations and procedures of the Member State which transmitted the data, bring an action or, if appropriate, a complaint before the competent authorities or courts of that State concerning the data relating to him or her recorded in the Central System, in order to exercise his or her rights under paragraph 5. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject in accordance with paragraph 13 shall subsist throughout the proceedings.~~

Article ~~30~~ 32

Supervision by the national supervisory authorities

1. ~~For the purposes laid down in Article 1(1) of this Regulation,~~ each Member State shall provide that ~~t~~The ~~national~~ supervisory authority or authorities ⌦ of each Member State ⌫ designated pursuant to Article ⇨ 41 ⇦ ~~28(1)~~ of Directive ~~95/46/EC~~ ⇨ referred to in Article [46(1)] of Regulation (EU) […/2016] ⇦ shall monitor ~~independently, in accordance with its respective national law,~~ the lawfulness of the processing~~, in accordance with this Regulation,~~ of personal data by the Member State in question ⌦ 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 fingerprint data.

Article ~~31~~ 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 ⌫ ~~the Agency~~, are carried out in accordance with Regulation (EC) No 45/2001 and with this Regulation.

2. The European Data Protection Supervisor shall ensure that an audit of the ~~Agency's~~ ⌦ 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 ⌫ ~~the Agency~~, and the national supervisory authorities. ~~The Agency~~ ⌦ eu-LISA ⌫ shall be given an opportunity to make comments before the report is adopted.

Article ~~32~~ 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(~~2~~1)(c) is carried out by an independent body, in accordance with Article ~~33(2)~~ 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 ~~40(7)~~ 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 ~~the Agency~~ ⌦ eu-LISA ⌫ every two years.

Article ~~33~~ 35

Protection of personal data for law enforcement purposes

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

~~2~~1. The ⌦ supervisory authority or authorities of each Member State referred to in Article [39(1)] of Directive [2016/… /EU] shall ⌫ monitor~~ing of~~ the lawfulness of the processing of personal data under this Regulation by the Member States for the purposes laid down in Article 1(~~2~~1)(c) of this Regulation, including their transmission to and from Eurodac~~, shall be~~

~~carried out by the national supervisory authorities designated pursuant to Framework Decision 2008/977/JHA~~.

~~3~~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.

~~4~~3. Personal data obtained pursuant to this Regulation from Eurodac for the purposes laid down in Article 1(~~2~~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.

~~5~~4. ⌦ Without prejudice to Article [23 and 24] of Directive [2016/ …/EU], ⌫ ~~T~~the Central System, the designated and verifying authorities and Europol shall keep records of the searches for the purpose of permitting the national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union data protection rules, including for the purpose of maintaining records in order to prepare the annual reports referred to in Article ~~40(7)~~ 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 ~~34~~ 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);

⇩ new

(e) prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);

↓ 603/2013 (adapted)

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

(~~f~~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);

(~~g~~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 ⌦ Chapter VI of of Regulation (EU) No. […/2016] ⌫ ~~Article 28 of Directive 95/46/EC~~] and in ⌦ Chapter VI ofArticle of Directive [2016/.../EU] ⌫ ⌦ Article [..] of Directive [2016/.../EU] ⌫ ~~25~~ of ~~Framework Decision~~ ~~2008/977/JHA~~ without delay at their request (personnel profiles);

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

(~~i~~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);

(~~j~~k) prevent the unauthorised reading, copying, modification or ~~erasure~~ ⌦ 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);

⇩ new

(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);

↓ 603/2013 (adapted)
⇨ new

(~~k~~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 ~~(j)~~ ⇨ (k) ⇦ that might indicate the occurrence of a security incident.

3. Member States shall inform ~~the Agency~~ ⌦ eu-LISA ⌫ of security incidents detected on their systems ⇨ without prejudice to the notification and communication of a personal data breach pursuant to [Articles 31 and 32] of Regulation (EU) No […/2016] respectively [Articles 28 and 29] ⇦ . ~~The Agency~~ ⌦ eu-LISA ⌫ shall inform the Member States,

Europol and the European Data Protection Supervisor in case of security incidents. The Member States concerned, ~~the Agency~~ ⌦ eu-LISA ⌫ and Europol shall collaborate during a security incident.

4. ~~The Agency~~ ⌦ 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 ~~35~~ 37

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

1. Personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of [Article […]~~2(b)~~ of Directive [2016/../EU] ~~Framework Decision 2008/977/JHA~~].

2. Personal data which originated in a Member State and are exchanged between Member States following a hit obtained for the purposes laid down in Article 1~~(2)~~(1)(c) shall not be transferred to third countries if there is a ~~serious~~ ⌦ 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.

⇩ new

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), particularly where that country is also the applicant's country of origin.

🡻 603/2013 (adapted)
⇨ new

~~3~~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] respectively with the national rules adopted pursuant to Directive [2016/…/EU] ⇦ to third countries to which Regulation (EU) No […/…] ~~604/2013~~ applies.

⇩ new

Article 38

Transfer of data to third countries for the purpose of return

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 Article 46 of Regulation (EU) No. […/2016], if necessary in

order to prove the identity of third-country nationals for the purpose of return, only where the following conditions are satisfied:

(b) the third country explicitly agrees to use the data only for the purpose for which they were provided and to what is lawful and necessary to secure the purposes laid down in Article 1(1)(b) and to delete that data where it is no longer justified to keep it;

(c) the Member State of origin which entered the data in the Central System has given its consent and the individual concerned has been informed that his or her personal information may be shared with the authorities of a third-country.

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), particularly where that country is also the applicant's country of origin.

3. A third-country shall not have direct access to the Central System to compare or transmit fingerprint 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.

↓ 603/2013 (adapted)
⇨ new

Article ~~36~~ 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~~(2)~~(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.

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

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

(b) the reasonable grounds given not to conduct comparisons with other Member States under Decision 2008/615/JHA, in accordance with Article ~~20~~ 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 ~~19(3)~~ 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~~ing non-~~personal data may be used for the monitoring and evaluation referred to in Article ~~40~~ 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 ~~duties~~ ⌦ tasks ⌫ .

Article ~~37~~ 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 ~~the Agency~~ ⌦ 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 [75 and 76] of Regulation (EU) […/2016] and Articles [52 and 53] of Directive [2016/… /EU] ⇦ .

~~CHAPTER VIII~~

~~*AMENDMENTS TO REGULATION (EU) NO 1077/2011*~~

~~*Article 38*~~

~~**Amendments to Regulation (EU) No 1077/2011**~~

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

~~(1) Article 5 is replaced by the following:~~

~~*"Article 5*~~

~~**Tasks relating to Eurodac**~~

~~In relation to Eurodac, the Agency shall perform:~~

~~(a) the tasks conferred on it by Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country~~

national or a stateless person), and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes[45]; and

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

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

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

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

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

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

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

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

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

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

"4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, is on the agenda.";»

(4) Article 17 is amended as follows:

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

"(g) without prejudice to Article 17 of the Staff Regulations, establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008 and Article 4(4) of Regulation (EU) No 603/2013;";»

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

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

(5) Article 19(3) is replaced by the following:

45 OJ L 180, 29.6.2013, p. 1.;

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

CHAPTER IX

FINAL PROVISIONS

Article ~~39~~ 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(~~2~~1)(c).

Article ~~40~~ 42

Annual report: monitoring and evaluation

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

⇩ new

4. By [*2020*] 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.

603/2013 (adapted) ⇨ new

~~4~~5. By ~~20 July 2018~~ ⇨ […] ⇦ and every four years thereafter, the Commission shall produce an overall evaluation of Eurodac, examining the results achieved against objectives and the impact on fundamental rights, including whether law enforcement access has led to indirect discrimination against persons covered by this Regulation, and assessing the continuing validity of the underlying rationale and any implications for future operations, and shall make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

~~5~~6. Member States shall provide ~~the Agency~~ ⌦ eu-LISA ⌫ and the Commission with the information necessary to draft the annual report referred to in paragraph 1.

~~6~~7. ~~The Agency~~ ⌦ eu-LISA ⌫ , Member States and Europol shall provide the Commission with the information necessary to draft the overall evaluation provided for in paragraph ~~4~~ 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

~~7~~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 fingerprint data with Eurodac data for law enforcement purposes, containing information and statistics on:

– the exact purpose of the comparison, including the type of terrorist offence or serious criminal offence,

– grounds given for reasonable suspicion,

– the reasonable grounds given not to conduct comparison with other Member States under Decision 2008/615/JHA, in accordance with Article ~~20~~ 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.

~~8~~9. On the basis of Member States and Europol annual reports provided for in paragraph ~~7~~ 8 and in addition to the overall evaluation provided for in paragraph ~~4~~ 5, the Commission shall compile an annual report on law enforcement access to Eurodac and shall transmit it to the European Parliament, the Council and the European Data Protection Supervisor.

Article ~~41~~ 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 ~~42~~ 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 ~~43~~ 45

Notification of designated authorities and verifying authorities

1. By ⇨ […] ⇦ ~~20 October 2013~~, each Member State shall notify the Commission of its designated authorities, of the operating units referred to in Article ~~5~~ 6(3) and of its verifying authority, and shall notify without delay any amendment thereto.

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

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

~~*Article 44*~~

~~**Transitional provision**~~

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

Article ~~45~~ 46

Repeal

Regulation ~~(EC) No 2725/2000 and Regulation (EC) No 407/2002 are~~ ⌦ (EU) No 603/2013 is ⌫ repealed with effect from ~~20 July 2015~~ ⇨ […] ⇦ .

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

Article ~~46~~ 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 ~~20 July 2015~~ ⇨ […] ⇦ .

⇩ new

Articles 2(2), 32, 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 91(2) of Regulation (EU) […/2016]. 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 62(1) of Directive [2016/ …/EU]. 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.

🡻 603/2013 (adapted)
⇨ new

Member States shall notify the Commission and ~~the Agency~~ ⌦ eu-LISA ⌫ as soon as they have made the technical arrangements to transmit data to the Central System ⌦ under Articles XX-XX ⌫ , ~~and in any event~~ no later than ~~20 July 2015~~ ⇨ […] ⇦ .

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

Done at Brussels,

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

↓ 603/2013

~~ANNEX I~~

~~*DATA FORMAT AND FINGERPRINT FORM*~~

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

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

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

~~**Norm for Member State identification letters**~~

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

↓ 603/2013 (adapted)

~~ANNEX II~~

~~*Repealed Regulations (referred to in Article 45)*~~	
~~Council Regulation (EC) No 2725/2000~~	~~(OJ L 316, 15.12.2000, p. 1.)~~
~~Council Regulation (EC) No 407/2002~~	~~(OJ L 62, 5.3.2002 p. 1.)~~

↓ 603/2013 (adapted)

~~ANNEX III~~

~~CORRELATION TABLE~~

~~Regulation (EC) No 2725/2000~~	~~This Regulation~~
~~Article 1(1)~~	~~Article 1(1)~~
~~Article 1(2), first subparagraph, points (a) and (b)~~	~~Article 3(1)(a)~~
~~Article 1(2), first subparagraph, point (c)~~	~~—~~
~~Article 1(2), second subparagraph~~	~~Article 3(4)~~
~~Article 1(3)~~	~~Article 1(3)~~
~~Article 2(1)(a)~~	~~—~~
~~Article 2(1)(b) to (e)~~	~~Article 2(1)(a) to (d)~~
~~—~~	~~Article 2(1)(e) to (j)~~
~~Article 3(1)~~	~~—~~
~~Article 3(2)~~	~~Article 3(3)~~
~~Article 3(3)(a) to (e)~~	~~Article 8(1)(a) to (e)~~
~~—~~	~~Article 8(1)(f) to (i)~~
~~Article 3(4)~~	~~—~~
~~Article 4(1)~~	~~Article 9(1) and Article 3(5)~~
~~Article 4(2)~~	~~—~~
~~Article 4(3)~~	~~Article 9(3)~~
~~Article 4(4)~~	~~Article 9(4)~~
~~Article 4(5)~~	~~Article 9(5)~~
~~Article 4(6)~~	~~Article 25(4)~~
~~Article 5(1), points (a) to (f)~~	~~Article 11, points (a) to (f)~~

~~—~~	~~Article 11, points (g) to (k)~~
~~Article 5(1), points (g) and (h)~~	~~—~~
~~Article 6~~	~~Article 12~~
~~Article 7~~	~~Article 13~~
~~Article 8~~	~~Article 14~~
~~Article 9~~	~~Article 15~~
~~Article 10~~	~~Article 16~~
~~Article 11(1) to (3)~~	~~Article 17(1) to (3)~~
~~Article 11(4)~~	~~Article 17(5)~~
~~Article 11(5)~~	~~Article 17(4)~~
~~Article 12~~	~~Article 18~~
~~Article 13~~	~~Article 23~~
~~Article 14~~	~~—~~
~~Article 15~~	~~Article 27~~
~~Article 16~~	~~Article 28(1) and (2)~~
~~—~~	~~Article 28(3)~~
~~Article 17~~	~~Article 37~~
~~Article 18~~	~~Article 29(1), (2), (4) to (10) and (12) to (15)~~
~~—~~	~~Article 29(3) and (11)~~
~~Article 19~~	~~Article 30~~
~~—~~	~~Articles 31 to 36~~
~~Article 20~~	~~—~~
~~Article 21~~	~~Article 39(1) and (2)~~
~~Article 22~~	~~—~~
~~Article 23~~	~~—~~
~~Article 24(1) and (2)~~	~~Article 40(1) and (2)~~

—	~~Article 40(3) to (8)~~
~~Article 25~~	~~Article 41~~
~~Article 26~~	~~Article 42~~
—	~~Articles 43 to 45~~
~~Article 27~~	~~Article 46~~

~~Regulation 407/2002/EC~~	~~This Regulation~~
~~Article 2~~	~~Article 24~~
~~Article 3~~	~~Article 25(1) to (3)~~
—	~~Article 25(4) and (5)~~
~~Article 4~~	~~Article 26~~
~~Article 5(1)~~	~~Article 3(3)~~
~~Annex I~~	~~Annex I~~
~~Annex II~~	—

↑

ANNEX

CORRELATION TABLE

Regulation (EU) No 603/2013	This Regulation
Article 1(1)	Article 1(1)(a) and (b)
Article 1(2)	Article 1(1)(c)
Article 1(3)	-
-	Article 1(3)
-	Article 2(1) to (4)
Article 2(1), introductory wording	Article 3(1), introductory wording
Article 2(1)(a) and (b)	Article 3(1)(a) and (b)
-	Article 3(1)(c)
Article 2(1)(c)	Article 3(1)(d)
Article 2(1)(d)	Article 3(1)(e)
Article 2(1)(e)	Article 3(1)(f)
Article 2(1)(f)	Article 3(1)(g)
Article 2(1)(g)	Article 3(1)(h)
Article 2(1)(h)	Article 3(1)(i)
Article 2(1)(i)	Article 3(1)(j)
Article 2(1)(j)	Article 3(1)(k)
Article 2(1)(k)	Article 3(1)(l)
Article 2(1)(l)	Article 3(1)(m)
-	Article 3(1)(n)
-	Article 3(1)(0)
Article 2(2), (3) and (4)	Article 3(2), (3) and (4)
Article 3(1) to (4)	Article 4(1) to (4)
Article 3(5)	Article 2(5)

-	Article 4(5)
Article 4(1), first and second subparagraph	Article 5(1)
Article 4(1), third subparagraph	Article 5(2)
Article 4(2)	Article 5(3)
Article 4(3)	Article 5(4)
Article 4(4)	Article 5(5)
Article 5	Article 6
Article 6	Article 7
Article 7	Article 8
Article 8(1)(a) to(i)	Article 9(1)(a) to (i)
-	Article 9(1)j) and (h)
Article 8(2)	Article 9(2)
-	Article 9(3)
Article 9(1)	Article 10(1)
Article 9(2)	Article 10(2)
Article 9(3)	-
Article 9(4)	-
Article 9(5)	-
-	Article 10(6)
Article 10(a) and (b)	Article 11(a) and (b)
Article 10(c)	Article 11(c)
Article 10(d)	Article 11(d)
Article 10 (e)	Article 11(e)
Article 11(a)	Article 12(a)
Article 11(b)	Article 12(b)
Article 11(c)	Article 12(c)
Article 11(d)	Article 12(d)
Article 11(e)	Article 12(e)

Article 11(f)	Article 12 (f)
Article 11(g)	Article 12(g)
Article 11(h)	Article 12(h)
Article 11(i)	Article 12(i)
Article 11(j)	Article 12(j)
Article 11 (k)	Article 12(k)
-	Article 12(l)
-	Article 12(m)
-	Article 12(n)
-	Article 12(0)
-	Article 12(p)
-	Article (q)
-	Article 12(r)
-	Article 12(s)
Article 12	-
Article 13	-
Article 14(1)	Article 13(1)
Article 14(2)	Article 13(2)
Article 14(2)(a)	Article 13(2)(a)
Article 14(2)(b)	Article 13(2)(b)
Article 14(2)(c)	Article 13(2)(c)
Article 14(2)(d)	Article 13(2)(d)
Article 14(2)(e)	Article 13(2)(e)
Article 14(2)(f)	Article 13(2)(f)
Article 14(2)(g)	Article 13(2)(g)
-	Article 13(2)(h)
-	Article 13(2)(i)
-	Article 13(2)(j)

-	Article 13(2)(k)
-	Article 13(2)(l)
-	Article 13(2)(m)
Article 14(3)	Article 13(3)
Article 14(4)	Article 13(4)
Article 14(5)	Article 13(5)
-	Article 13(6)
-	Article 13(7)
-	
Article 15	-
Article 16	-
Article 17(1)	Article 14(1)
Article 17(1)(a)	-
Article 17(1)(b)	-
Article 17(1(c)	-
Article 17(2)	Article 14(2)
-	Article 14(2)(a)
	Article 14(2)(b)
	Article 14(2)(c)
	Article 14(2)(d)
	Article 14(2)(e)
	Article 14(2)(f)
	Article 14(2)(g)
	Article 14(2)(h)
	Article 14(2)(i)
	Article 14(2)(j)
	Article 14(2)(k)
	Article 14(2)(l)

	Article 14(2)(m)
Article 17(3)	Article 14(3)
Article 17(4)	Article 14(4)
Article 17(5)	Article 14(5)
-	Article 14(6)
-	Article 15(1)
-	Article 15(2)
-	Article 15(3)
-	Article 15(4)
-	Article 16(1) to (5)
-	Article 17(1)
-	Article 17(2)
-	Article 17(3)
-	Article 17(4)
-	Article 18(1)
-	Article 18(2)
Article 18(1)	Article 19(1)
Article 18(2)	Article 19(2)
Article 19(3)	Article 19(3)
-	Article 19(4)
-	Article 19(5)
Article 19(1)	Article 20(1)
Article 19(2)	Article 20(2)
Article 19(3)	Article 20(3)
Article 19(4)	Article 20(4)
-	Article 20(5)
Article 20(1)	Article 21(1)
Article 20(1)(a) to (c)	Article 21(a) to (c)

Article 20(2)	Article 21(2)
Article 21(1)(a) to (c)	Article 22(1)(a) to (c)
Article 21(2)	Article 22(2)
Article 21(3)	Article 22(3)
Article 22(1)	Article 23(1)
Article 22(2)	Article 23(2)
Article 23(1)(a) to (e)	Article 24(1)(a) to (e)
Article 23(2)	Article 24(2)
Article 23(3)	Article 24(3)
Article 23(4)(1)to (c)	Article 24(4)(1) to (c)
Article 24	Article 25
Article 25(1) to (5)	Article 26(1) to (6)
-	Article 26(6)
Article 26	Article 27
Article 27	Article 28
Article 28	Article 29
Article 29(1) to (e)	Article 30 (1) to (e)
-	Article 30(1)(f)
-	Article 30(1)(g)
Article 29(2)	Article 30(2)
Article 29(3)	Article 30(3)
Article 29(4) to (15)	-
-	Article 31(1)
-	Article 31(2)
-	Article 31(3)
-	Article 31(4)
-	Article 31(5)
-	Article 31(6)

-	Article 31(7)
-	Article 31(8)
Article 30	Article 32
Article 31	Article 33
Article 32	Article 34
Article 33(1)	Article 35(1)
Article 33(2)	Article 35(2)
Article 33(3)	Article 35(3)
Article 33(4)	Article 35(4)
Article 33(5)	-
Article 34(1)	Article 36(1)
Article 34(2)(a) to (k)	Article 36(2)(a) to (k)
-	Article 36(2)(1) to (n)
Article 34(3)	Article 36(3)
Article 34(4)	Article 36(4)
Article 35(1)	Article 37(1)
Article 35(2)	Article 37(2)
Article 35(3)	Article 37(3)
-	Article 37(4)
-	Article 38(1)
-	Article 38(2)
-	Article 38(3)
Article 36(1)	Article 39(1)
Article 36(2)(a) to (h)	Article 39(2)(a) to (h)
Article 36 (3)	Article 39(3)
Article 37	Article 40
Article 38	-
Article 39	Article 41

Article 40(1)	Article 42(1)
Article 40(2)	Article 42(2)
Article 40(3)	Article 42(3)
Article 40(4)	Article 42(4)
Article 40(5)	Article 42(5)
Article 40(6)	Article 42(6)
Article 40(7)	Article 42(7)
Article 40(8)	Article 42(8)
-	Article 42(9)
Article 41	Article 43
Article 42	Article 44
Article 43	Article 45
Article 44	-
Article 45	Article 46
Article 46	Article 47
Annex I	Annex I
Annex II	-
Annex III	Annex II

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

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 irregular 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 (recast)

1.2. Policy area(s) concerned in the ABM/ABB structure[46]

Policy area: Migration and Home Affairs (title 18)

Activity: Asylum and Migration

1.3. Nature of the proposal/initiative

☐ The proposal/initiative relates to **a new action**

☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**[47]

☒ The proposal/initiative relates to **the extension of an existing action**

☐ The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objective(s)

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

In the European Agenda on Migration (COM(2015)240 final) the Commission announced that it will have to evaluate the Dublin system and determine whether a revision of the legal parameters of Dublin will be needed to achieve a fairer distribution of asylum seekers in Europe. The Commission also proposed to look into the possibility of adding additional biometric identifiers to EURODAC, such a facial images and the use of facial recognition software.

The refugee crisis has exposed significant structural weaknesses and shortcomings in the design and implementation of European asylum and migration policy, including the Dublin and EURODAC systems, which prompted calls for reform.

On 6 April in its Communication "Towards a reform of the Common European Asylum System and enhancing legal avenues to Europe" (COM(2016) 197 final) the Commission considered it a priority to bring forward a reform of the Dublin Regulation and establish a sustainable and fair system for determining the Member State responsible for asylum seekers ensuring a high degree of solidarity and a fair sharing of responsibility between Member States by proposing a corrective allocation mechanism.

As part of this, the Commission considered that EURODAC should be reinforced to reflect changes to the Dublin mechanism and to make sure that it continues to provide the fingerprint evidence it needs to function. It was also considered that EURODAC could

46 ABM: activity-based management; ABB: activity-based budgeting.

47 As referred to in Article 54(2)(a) or (b) of the Financial Regulation.

contribute to the fight against irregular migration by storing fingerprint data under all categories and allowing comparisons to be made with all stored data for that purpose.

1.4.2. Specific objective(s) and ABM/ABB activity(ies) concerned

DG HOME AMP Specific objective No 1: To strengthen and develop all aspects of the Common European Asylum System, including its external dimension.

ABM/ABB activity(ies) concerned: Activity 18 03: Asylum and Migration.

Specific objective No 1: Eurodac functional system evolution

Specific objective No 2: Eurodac database capacity upgrade

1.4.3. Expected result(s) and impact

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

The proposal will aim to enhance the identification of irregular third-country nationals within the EU as well as to ensure the effective implementation of the revised Dublin Regulation by providing fingerprint evidence to determine the Member State responsible for examining an application of international protection.

This proposal aims to assist Member States to ensure that an applicant for international protection will have their application examined by a single Member State and will reduce the scope of abuse of the asylum system by deterring "asylum shopping" within the EU.

Member States will also benefit from being able to identify irregular third-country nationals illegally staying in the EU by storing their personal data and indicating the first country through which they entered or where they may also been staying illegally. The information stored at EU level will in turn assist a Member State to re-document a third-country national with a view to returning them to their country of origin or a third-country to which they will be readmitted.

Many applicants for international protection and third-country nationals arriving irregularly to the European Union travel with families and in many cases with very young children. Being able to identify these children with the help of fingerprints and facial images will help to identify them in cases where they are separated from their families by allowing a Member State to follow up a line of inquiry where a fingerprint match indicates that they were present in another Member State. It would also strengthen the protection of unaccompanied minors who do not always formally seek international protection and who abscond from care institutions or child social services to which their care has been assigned. Under the current legal and technical framework their identity cannot be established. Thus the EURODAC system could be used to register children from third-countries where they are found undocumented within the EU to help keep track of them and prevent them from ending up in scenarios of exploitation.

1.4.4. Indicators of results and impact

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

<u>During the upgrading of the Central System</u>

After the approval of the draft proposal and the adoption of the technical specifications the recast EURODAC Central System will be upgraded in terms of capacity and througput for transmission from the Member States' National Access Points. eu-LISA will coordinate the project management of upgrading the Central System and the national systems at EU level and the integration of the National Uniform Interface (NUI) carried out by Member States at national level.

Specific Objective: Ready for operations when the amended Dublin Regulation will go live.

Indicator: In order to go live, eu-LISA has notified the successful completion of a comprehensive test of the EURODAC Central System which shall be conducted by the Agency together with the Member States.

<u>Once the new Central System is operational</u>

Once the EURODAC system is operational eu-LISA shall ensure that systems are in place to monitor the functioning of the system against objectives. At the end of each year eu-LISA should submit to the European Parliament, the Council and the Commission a 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 its objectives.

By 2020, eu-LISA should conduct a study on the technical feasibility of adding facial recognition software to the Central System that ensures reliable and accurate results following a comparison of facial image data.

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

Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement purposes, containing statistics on the number of requests made and hits received.

1.5. Grounds for the proposal/initiative

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

(1) Determining the Member State responsible under the amended Dublin Regulation proposal.

(2) Control the identity of irregular third-country nationals to and within the EU for the purposes of re-documentation and return and identifying vulnerable third-country nationals such as children who often fall victim to smuggling.

(3) The fight against international criminality, terrorism and other security threats is reinforced.

1.5.2. Added value of EU involvement

No Member State alone is able to cope on its own with irregular immigration or deal with all the asylum applications made within the EU. As has been witnessed in the EU for many years, a person may gain entry to the EU via the external borders, but not declare themselves at a designated border crossing point. This has been the case in particular in 2014-2015 where over one million irregular migrants arrived to the EU via the Central and Southern Mediterranean routes. Similarly, 2015 witnessed onward movements from those countries situated at the external borders to other Member States. The monitoring of compliance with EU rules and procedures such as the Dublin procedure therefore cannot be done by Member States acting alone. In an area without internal borders, action against irregular immigration should be undertaken in common. Considering all this, the EU is better placed than Member States to take the appropriate measures.

The use of the three existing EU large-scale IT systems (SIS, VIS and Eurodac) brings benefits to border management. Better information on cross border movements of third country nationals at EU level would help establish a factual basis to develop and adapt the EU migration policy. Therefore, an amendment of the EURODAC Regulation is also required in order to add an additional purpose thereto, namely allow access for the purpose of controlling illegal migration to and secondary movements of irregular migrants within the EU. This objective cannot be sufficiently achieved by the Member States on their own, since such amendment can only be proposed by the Commission.

1.5.3. Lessons learned from similar experiences in the past

The main lessons learnt from upgrading the Central System following the adoption of the first recast EURODAC Regulation[48] was the importance of early project management by Member States and ensuring that the project of upgrading the national connection was managed against milestones. Even though a rigid project management schedule was set by eu-LISA for both upgrading the Central System and Member States national connections, a number of Member States failed or risked connecting to the Central System by 20 July 2015 (two years after adoption of the Regulation).

In the Lessons Learnt workshop following the upgrading of the Central System in 2015, Member States also flagged that a roll-out phase was needed for the next upgrade of the Central System to ensure that all Member States could manage to connect to the Central System on time.

Alternative solutions were found for those Member States that were late to connect to the Central System in 2015. These included eu-LISA lending a National Access Point/ Fingerprint Image Transmission (NAP/FIT) solution to one Member State that was used for testing simulations by the Agency, because the Member State in question had failed to secure the necessary funding to begin their procurement procedure shortly after the adoption of the EURODAC Regulation. Two other Member States had to resort to using an 'in-house' solution for their connection before installing their procured NAP/FIT solutions.

The use of a Framework Contract to provide functionalities and provision of maintenance services for the EURODAC system was established by eu-LISA and an external Contractor. Many Member States used this framework contract to procure a standardised NAP/FIT solution, which was deemed to have made savings and avoided the need for national procurement procedures. A framework contract of this sort should be considered again for the future upgrade.

1.5.4. Compatibility and possible synergy with other appropriate instruments

This proposal should be seen as part of the continuous development of the Dublin Regulation[49], the Commission's Communication "Towards a reform of the Common European Asylum System and enhancing legal avenues to Europe"[50], and in particular the Commission's Communication on Stronger and Smarter Information Systems for Borders and Security[51], as well as in conjunction with the ISF borders[52], as part of the MFF and the establishing Regulation of eu-LISA[53].

48 OJ L 180, 29.6.2013, p.1

49 Regulation (Eu) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast). OJ L 180, 29.6.2013, p31.

50 COM(2016) 197 final.

51 COM(2016) 205 final

52 Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC, OJ L150, 20.5.2014, p.143

53 Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. Article 1.3 "The Agency may also be made responsible for the preparation, development and operational management of large-scale IT systems in the area of freedom, security and justice other than those referred to in paragraph 2, only if so provided by relevant legislative instruments…", OJ L 286, 1.11.2011, p. 1–17

Within the Commission DG HOME is the Directorate General responsible for the establishment of EURODAC.

1.6. Duration and financial impact

☐ Proposal/initiative of **limited duration**

– ☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY

☒ Proposal/initiative of **unlimited duration**

– Implementation with a start-up period from 2017 to 2020,

– followed by full-scale operation.

1.7. Management mode(s) planned[54]

☒ **Direct management** by the Commission through

– ☒ by its departments, including by its staff in the Union delegations;

– ☐ executive agencies

☐ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

☐ international organisations and their agencies (to be specified);

☐the EIB and the European Investment Fund;

☒ bodies referred to in Articles 208 and 209;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

Comments

The Commission will be responsible for the overall management of the action and eu-LISA will be responsible for the development, operation and maintenance of the system.

[54] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The rules on monitoring and evaluation of the Eurodac system are foreseen in Article 40 of the proposal:

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.

3a. By [2020] 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.

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

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

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

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

— the exact purpose of the comparison, including the type of terrorist offence or serious criminal offence,

— grounds given for reasonable suspicion,

— the reasonable grounds given not to conduct comparison with other Member States under Decision 2008/615/JHA, in accordance with Article 20(1) of this Regulation,

— number of requests for comparison,

— the number and type of cases which have ended in successful identifications, and

— the need and use made of the exceptional case of urgency, including those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority.

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

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

2.2. Management and control system

2.2.1. Risk(s) identified

The following risks are identified:

1) Difficulties for eu-LISA to manage the development of this system in parallel to development related to other more complicated systems (Entry-Exit system, AFIS for SIS II, VIS, …) taking place within the same time period.

2) The upgrade Eurodac needs to be integrated with the national IT systems which need to be fully aligned with central requirements. The discussions with Member States to ensure uniformity in the usage of the system may introduce delays in the development.

2.2.2. Control method(s) envisaged

The Agency’s accounts will be submitted for the approval of the Court of Auditors, and subject to the discharge procedure. The Commission’s Internal Audit Service will carry out audits in cooperation with the Agency's internal auditor.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

The measures foreseen to combat fraud are laid down in Article 35 of Regulation (EU) 1077/2011 which provides as follows:

1. In order to combat fraud, corruption and other unlawful activities, Regulation (EC) No 1073/1999 shall apply.

2. The Agency shall accede to the Interinstitutional Agreement concerning internal investigations by the European Anti-Fraud Office (OLAF) and shall issue, without delay, the appropriate provisions applicable to all the employees of the Agency.

3. The decisions concerning funding and the implementing agreements and instruments resulting from them shall explicitly stipulate that the Court of Auditors and OLAF may carry out, if necessary, on-the-spot checks among the recipients of the Agency's funding and the agents responsible for allocating it.

In accordance with this provision, the decision of the Management Board of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice concerning the terms and conditions for internal investigation sin relation to the prevention of fraud, corruption and any illegal activity detrimental to the Union's interests was adopted on 28 June 2012.

DG HOME's fraud prevention and detection strategy will apply.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

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

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Heading 3 - Security and Citizenship	Diff./Non-diff.[55]	from EFTA countries [56]	from candidate countries[57]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
3	18.0303 – European fingerprint database (Eurodac)	Diff.	NO	NO	NO	NO
3	18.0207 – European Agnecy for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)	Diff.	NO	NO	YES*	NO

* eu-LISA receives contributions from the countries associated with the Schengen Agreement (NO, IS, CH, LI)

[55] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[56] EFTA: European Free Trade Association.

[57] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	3	Security and Citizenship

eu-LISA			Year **2017**[58]	Year **2018**	Year **2019**	Year **2020**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
Title 1: Staff expenditure	Commitments	(1)	0,268	0,268	0,268	0,268				**1,072**
	Payments	(2)	0,268	0,268	0,268	0,268				**1,072**
Title 2: Infrastructure and operating expenditure	Commitments	(1a)	0	0	0	0				**0**
	Payments	(2a)	0	0	0	0				**0**
Title 3: Operational expenditure *	Commitments	(3a)	11,330	11,870	5,600	0				**28,800**
	Payments	(3b)	7,931	8,309	3,920	8,640				**28,800**
TOTAL appropriations for eu-LISA	Commitments	=1+1a +3a	11,598	12,138	5,868	0,268				**29,872**
	Payments	=2+2a +3b	8,199	8,577	4,188	8,908				**29,872**

* The Impact assessment performed by eu-LISA foresees a continuous increase of the traffic rates as during the last months of 2015 before the border close along the west Balkan route.

* The potential costs for DubliNet upgrades and system operation are included in the Title 3 total.

58 Year N is the year in which implementation of the proposal/initiative starts.

Heading of multiannual financial framework	5	'Administrative expenditure'

EUR million (to three decimal places)

		Year 2017	Year 2018	Year 2019	Year 2020	Enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
DG: Migration and Home Affairs									
• Human Resources		0,402	0,402	0,402	0,402				**1,608**
• Other administrative expenditure									
TOTAL DG Migration and Home Affairs	Appropriations	0,402	0,402	0,402	0,402				**1,608**

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	0,402	0,402	0,402	0,402				**1,608**

EUR million (to three decimal places)

		Year 2017[59]	Year 2018	Year 2019	Year 2020	Enter as many years as necessary to show the duration of the impact (see point 1.6)			TOTAL
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	12,000	12,540	6,270	0,670				**31,480**
	Payments	8,601	8,979	4,590	9,310				**31,480**

There is no Europol related costs since Europol accesses Eurodac via the Dutch National Interface to Eurodac.

[59] Year N is the year in which implementation of the proposal/initiative starts.

3.2.2. Estimated impact on eu-LISA's appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ☒ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2017**		Year **2018**		Year **2019**		Year **2020**		Enter as many years as necessary to show the duration of the impact (see point 1.6)						**TOTAL**	
			OUTPUTS															
	Type[60]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[61] Eurodac functional system evolution																		
- Output	Contractor *			0,130		0,670		0		0								0,800
Subtotal for specific objective No 1				0,130		0,670		0		0								0,800
SPECIFIC OBJECTIVE No 2 Eurodac database capacity upgrade																		
- Output	Hardware, Software **			11,200		11,200		5,600		0								28,000
Subtotal for specific objective No 2				11,200		11,200		5,600		0								28,000
TOTAL COST				11,330		11,870		5,600		0								28,800

* All contractual costs for the functional updates are split between the first 2 years with the biggest part of the budget in the 2nd year (following acceptance)

** Capacity payments is split within the 3 years as 40%, 40%, 20%

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

61 As described in point 1.4.2. 'Specific objective(s)…'

3.2.3. Estimated impact on eu-LISA's human resources

3.2.3.1. Summary

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2017** [62]	Year **2018**	Year **2019**	Year **2020**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
Officials (AD Grades)	0,268	0,268	0,268	0,268				**1,072**
Officials (AST grades)								
Contract staff								
Temporary staff								
Seconded National Experts								
TOTAL	0,268	0,268	0,268	0,268				**1,072**

Estimated impact on the staff (additional FTE) – establishment plan of eu-LISA

Posts (establishment plan)	**2017**	**2018**	**2019**	**2020**
Baseline - Communication[63]	115	113	113	113
Additional posts	2	2	2	2
Additional posts EES	14	14	14	14
Total	131	129	129	129

62 Year 2017 is the year in which implementation of the proposal/initiative starts.

63 COM(2013) 519 final: Communication from the Commission to the European Parliament and the Council – Programming of human and financial resources for decentralised agencies 2014-2020.

Recruitment is planned for January 2017. All staff must be available as of early 2017 in order to allow starting the development in due time with a view of ensuring an entry into operations of Eurodac in 2017. The 2 new Temporary Agents (TAs) are needed to cover needs both for the project implementation as well as for operational support and maintenance after deployment to production. These resources will be used:

- To support the project implementation as project team members, including activities as: the definition of requirements and technical specifications, cooperation and support to MS during the implementation, updates of the Interface Control Document (ICD), the follow-up of the contractual deliveries, project testing activities (including MS test coordination), documentation delivery and updates etc.
- To support transition activities for putting the system into operations in cooperation with the contractor (releases follow-up, operational process updates, trainings (including MS training activities) etc.
- To support the longer term activities, definition of specifications, contractual preparations in case there is reengineering of the system (e.g. due to Image recognition) or in case the new Eurodac Maintenance in Working Order (MWO) contract will need to be amended to cover additional changes (from technical and budgetary perspective)
- To enforce the second level support following Entry into Operation (EiO), during continuous maintenance and operations.

It has to be noted that the two new resources (FTE TA) will act on top of the internal team capabilities which will be as well utilised for the project/contractual and financial follow-up/ operational activities. The use of TAs will provide adequate duration and continuity of the contracts to ensure business continuity and use of the same specialized people for operational support activities after the project conclusion. On top the operational support activities require access to Production environment that cannot be assigned to contractors or external staff.

3.2.3.2. Estimated requirements of human resources for the parent DG

– ☐ The proposal/initiative does not require the use of human resources.

– ☒ The proposal/initiative requires the use of human resources, as explained below:

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

	Year **2017**	Year **2018**	Year **2019**	Year **2020**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			**TOTAL**
• **Establishment plan posts (officials and temporary staff)**								
18 01 01 01 (Headquarters and Commission's Representation Offices)	0,402	0,402	0,402	0,402				1,608
XX 01 01 02 (Delegations)								

XX 01 05 01 (Indirect research)									
10 01 05 01 (Direct research)									
• **External staff (in Full Time Equivalent unit: FTE)**[64]									
XX 01 02 01 (AC, END, INT from the 'global envelope')									
XX 01 02 02 (AC, AL, END, INT and JED in the Delegations)									
XX 01 04 ***yy***[65]	- at Headquarters[66]								
	- in Delegations								
XX 01 05 02 (AC, END, INT – Indirect research)									
10 01 05 02 (AC, END, INT – Direct research)									
Other budget lines (specify)									
TOTAL		0,402	0,402	0,402	0,402				1,608

18 is the policy area or budget title concerned.

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

Description of tasks to be carried out:

Officials and temporary staff	Various tasks in relation to Eurodac, e.g. in the context of Commission opinion on the annual work programme and monitoring of its implementation, supervision of the preparation of the Agency's budget and monitoring of its implementation, assisting the Agency in developing its activities in line with EU policies including by participating in experts meetings, etc.
External staff	

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

64 AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JED = Junior Experts in Delegations.

65 Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

66 Mainly for the Structural Funds, the European Agricultural Fund for Rural Development (EAFRD) and the European Fisheries Fund (EFF).

3.2.4. Compatibility with the current multiannual financial framework

– ☒ The proposal/initiative is compatible the current multiannual financial framework. ☐ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

– ☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[67].

3.2.5. Third-party contributions

– ☒ The proposal/initiative does not provide for co-financing by third parties.

– ☐ The proposal/initiative provides for the co-financing estimated below:

EUR million (to three decimal places)

	Year **2017**	Year **2018**	Year **2019**	Year **2020**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[67] See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

3.3. Estimated impact on revenue

– ☐ The proposal/initiative has no financial impact on revenue.

– ☒ The proposal/initiative has the following financial impact:

☐ on own resources

☒ on miscellaneous revenue

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[68]						
		Year **2017**	Year **2018**	Year **2019**	Year **2020**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….		0,492	0,516	0,243	0,536			

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

Specify the method for calculating the impact on revenue.

The budget shall include a contribution from countries associated with the Eurodac related measures as laid down in the respective agreements *. The estimates provided are purely indicative and are based on calculations for revenues for the implementation of the Eurodac system from the States that currently contribute the general budget of the European Union (consumed payments) an annual sum for the relevant financial year, calculated in accordance with its gross domestic product as a percentage of the gross domestic product of all the participating States. The calculation is based on June 2015 figures from EUROSTAT which are subject to considerable variation depending on the economic situation of the participating States.

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

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

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

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

[68] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 25 % for collection costs.