Council of the
European Union

Brussels, 9 February 2024
(OR. en)

6366/24

Interinstitutional File:
2016/0132(COD)

ASILE 19
EURODAC 3
ENFOPOL 56
IXIM 42
CODEC 380

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	6060/24
No. Cion doc.:	11205/20 + ADD 1; COM(2020) 614 final.
Subject:	Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) No 604/2013 and Directive 2001/55/EC, 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 Regulations (EU) 2018/1240, (EU) 2019/818 and (EU) 2017/2226 - Letter to the Chair of the LIBE Committee of the European Parliament

Following the Permanent Representatives Committee meeting of 8 February 2024 which endorsed the final compromise text on the above-mentioned proposal with a view to agreement, delegations are informed that the Presidency sent the attached letter, together with its Annexes, to the Chair of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE).

Council of the European Union

SGS 24 / 000802

Brussels, 08/02/2024

Mr. Juan Fernando LÓPEZ AGUILAR
Chair of the Committee on Committee on Civil Liberties, Justice and Home Affairs
European Parliament
Rue Wiertz 60
B-1047 BRUSSELS

Subject: Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], 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 Regulations (EU) 2018/1240 and (EU) 2019/818

Dear Mr. LÓPEZ AGUILAR,

Following the informal negotiations on this proposal between the representatives of the three institutions, today the Permanent Representatives Committee agreed with the final compromise text.

I am therefore now in a position to inform you that, should the European Parliament adopt its position at first reading, in accordance with Article 294(3) TFEU, in the exact form of the text set out in the Annex to this letter (subject to revision by the lawyer-linguists of the two institutions), the Council, in accordance with Article 294(4) TFEU, will approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the position of the European Parliament.

On behalf of the Council, I also wish to thank you for your close cooperation which should enable us to reach agreement on this file at first reading.

Yours sincerely

Willem van de Voorde
Chairman of the
Permanent Representatives Committee

Copy:
- Ms Ylva JOHANSSON, European Commissioner for Home Affairs
- Mr Jorge BUXADÉ VILLALBA, European Parliament rapporteur

Rue de la Loi/Wetstraat 175 – 1048 Bruxelles/Brussel – Belgique/België
Tél./Tel. +32 (0)2 281 61 11

REGULATION (EU) 2024/…
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of …

on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) ▌…/… [Regulation on Asylum and Migration Management] ▌, of Regulation (EU) ▌…/… [Resettlement Regulation], ***and Directive 2001/55/EC [Temporary Protection Directive],*** **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 Regulations (EU) 2018/1240***,* **and (EU) 2019/818**

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)***(c),*** (d), (e) and (g), 79(2)(c), 87(2)(a) and 88(2)(a) thereof,

Having regard to the proposal from the European Commission,

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

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

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

▌

(1) 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.

(2) For the purposes of applying Regulation (EU) …/… [▌ Asylum and Migration Management] ***establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection registered in one of the Member States by a third-country national or a stateless person***, it is necessary to establish the identity of applicants for international protection and of persons apprehended in connection with the ***irregular*** crossing of the external borders of the Union. It is also desirable, in order effectively to apply Regulation (EU) …/… [▌ Asylum and Migration Management], and in particular ***Article 26(1)(b)*** 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.

(3) Moreover, for the purposes of effectively applying Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] and in accordance with the rules thereof, it is necessary to clearly mark in Eurodac the fact that there has been a shift of responsibility between Member States, including in cases of relocation. ▌

▌

(4) It is also necessary, in order to effectively apply Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] or to identify any secondary movements to allow each Member State to check whether a third-country national or a stateless person ***found*** illegally staying on its territory or who applies for international protection has been ***granted international protection or a national humanitarian status*** by another Member State in accordance with Regulation (EU) …/… [Resettlement Regulation] or in accordance with a national resettlement scheme. For that purpose, the biometric data of persons registered for the purpose of conducting an admission procedure should be stored in Eurodac ***as soon as the international protection or humanitarian status under national law is granted, and no later than 72 hours thereafter***.

(5) ***In order to smoothly apply*** Regulation (EU) …/… [Resettlement Regulation], it is necessary to ▌ allow each Member State to check whether a third-country national or a stateless person has been ***granted international protection or a national humanitarian status in accordance with Regulation (EU) …/… [Resettlement Regulation]*** by another Member State or has been admitted to the territory of the Member States in accordance with a national resettlement scheme. In order to be able to apply the refusal grounds provided for under ***Article 6(1)(e) and (f) as well as Article 6(2)(a) of*** Regulation (EU) …/… [Resettlement Regulation] within the context of a new admission procedure, Member States also need information on the conclusion of previous admission procedures as well as information on any decision on granting international protection or a humanitarian status under national law. Information on the ***decision on granting international protection or a national humanitarian status*** is furthermore needed to identify the Member State that concluded the procedure and thus to enable Member States to seek supplementary information from that Member State.

(6) Furthermore, in order to reflect accurately the obligations Member States have under international law to conduct search and rescue operations and to provide a more accurate picture of the composition of migratory flows in the EU it is also necessary to record in Eurodac the fact that the third-country nationals or stateless persons were disembarked following search and rescue operations, including for statistical purposes. Without prejudice to the application of Regulation (EU) …/… [Regulation on Asylum and Migration Management], the recording of this fact should not result in any difference of treatment of persons registered in Eurodac upon apprehension in connection with the irregular crossing of an external border. This should be without prejudice to the respect of rules under EU law applicable to third-country nationals or stateless persons disembarked following search and rescue operations.

(7) ***Furthermore, for the purposes of supporting the asylum system by applying Regulation (EU) …/… [Asylum and Migration Management Regulation], Regulation (EU) …/… [Asylum Procedure Regulation], Regulation (EU) …/… [Qualification Regulation] and Directive (EU) …/… [Reception Conditions Directive] it is necessary to record whether, following security checks referred to in this Regulation, it appears that a person could pose a threat to internal security. That recording should be carried out by the Member State of origin defined in this Regulation. The existence in Eurodac of such a record is without prejudice to the requirement of an individual examination in order to apply Article 12, Article 14(1) points (d) or (e) or Article 19(1) point (b) of Regulation (EU) …/… [Qualification Regulation] and Regulation (EU) …/… [Asylum Procedures Regulation]. The record should be erased if the investigation shows that there are insufficient grounds to consider that the person represents a threat to internal security.***

(8) Following the security checks referred to in this Regulation, the fact that the person could pose a threat to internal security ('security flag') should only be recorded in Eurodac if the person is violent or unlawfully armed, or where there are clear indications that the person is involved in any of the offences referred to in Directive (EU) 2017/541 or in any of the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA. When assessing whether a person is unlawfully armed, it is necessary that a Member State determine whether the person is carrying a firearm without a valid permit or authorisation, or any other type of prohibited weapon as defined under national law. When assessing whether a person is violent, it is necessary that a Member State determine whether the person has displayed behaviour that results in physical harm to other persons, that would amount to a criminal offences under national law.

(9) Council Directive 2001/55/EC[1] provides for a system of temporary protection which has been activated for the first time by Council Implementing Decision (EU) 2022/382 in response to the war in Ukraine. Pursuant to that temporary protection regime Member States are to register persons enjoying temporary protection on their territory. Member States are also required, inter alia, to reunite family members and to cooperate with each other with regard to the transferral of the residence of persons enjoying temporary protection from one Member State to another. It is appropriate to supplement the data collection provisions of Drective 2001/55/EC by including persons benefiting from temporary protection in Eurodac. In this regard, biometric data are an important element in establishing such persons' identity or family relationships, and thus protecting a substantial public interest within the meaning of Article 9(2)(g) of Regulation (EU) 2016/679. Moreover, by including the biometric data of beneficiaries of temporary protection in Eurodac rather than in a peer-to-peer system between Member States, such persons will benefit from the safeguards and protections laid down in this Regulation particularly with regard to data retention periods, which should be as short as possible.

---

[1] ***Council Directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between Member States in receiving such persons and bearing the consequences thereof (OJ L 212, 7.8.2001, p. 12).***

(10) However, in view of the fact that a platform has already been set up by the Commission, in cooperation with eu-LISA and the Member States, to deal with the information exchanges necessary pursuant to Directive 2001/55/EC, it is appropriate to exclude from Eurodac those persons benefiting from temporary protection pursuant to Council Implementing Decision (EU) 2022/382, and the national measures taken pursuant thereto. Such exclusion should also apply in respect of any future amendments to Council Implementing Decision (EU) 2022/382 and any extensions thereto.

(11) It is appropriate to defer the application of Article 26 to three years after the entry into application of the other provisions of this Regulation, in order to ensure sufficient time for an assessment by the Commission of the functioning and the operational efficiency of any IT system used to exchange the data of the beneficiaries of temporary protection and of the expected impact of applying this Article in case of a future activation of Council Directive 2001/55/EC.

(12) Biometrics constitute an important element in establishing the exact identity of the persons falling under the scope of this Regulation because they ensure high accuracy of identification. It is necessary to set up a system for the comparison of their biometric data.

(13) It is also necessary to ▌ ensure ***that*** that system ***functions*** within the interoperability framework established by Regulations (EU) 2019/817[2] and (EU) 2019/818[3] of the European Parliament and of the Council ***in accordance with this Regulation and Regulation (EU) 2016/679 of the European Parliament and of the Council[4], in particular with the principles of necessity, proportionality and purpose limitation set out in that Regulation.***

(14) The reuse by Member States of the biometric data of third-country nationals or stateless persons already taken pursuant to this Regulation for the purposes of transmission to Eurodac in accordance with the conditions set out in this Regulation should be encouraged.

---

2 Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

3 Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

4 ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).***

(15) Furthermore, it is necessary to introduce the provisions that would frame the access of European Travel Information and Authorization System (ETIAS) national units and of competent visa authorities to Eurodac in accordance with Regulation (EU) 2018/1240[5] and (EC) No 767/2008[6] of the European Parliament and of the Council.

(16) ***For*** the purpose of ***assisting with the control of*** irregular ***immigration and of providing statistics supporting evidence-based policy making,*** eu-LISA ***should be able*** to produce cross-system statistics using data from Eurodac, the Visa Information System, ETIAS and the Entry/Exit System ***(EES)***[7]. In order to specify the content of these cross-system statistics, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers.

---

5 Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

6 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

7 ***Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 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 and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).***

(17) To those ends, it is necessary to set up a system known as 'Eurodac', consisting of a Central System and of the Common Identity Repository ***(CIR)*** established by Regulation (EU) 2019/818▌, which will operate a computerised central database of biometric data, ***alphanumeric data and, where available, a scanned colour copy of an identity or travel document,*** as well as of the electronic means of transmission between ***Eurodac*** and the Member States, hereinafter the 'Communication Infrastructure'.

▌

(18) The Communication of the Commission of 13 May 2015, titled 'A European Agenda on Migration'[8] 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).

(19) For the purposes of obtaining high accuracy identification, fingerprints should always be preferred over facial images. To this end, 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. To assist Member States overcome challenges, where it is impossible to take the fingerprints of the third-country national or stateless person because his or her fingertips are damaged, either intentionally or not, or amputated, this Regulation should permit the comparison of a facial image without fingerprints.

[8] COM(2015) 240 final, 13.5.2015

(20) The return of third-country nationals or stateless persons who do not have a right to stay in the Union, in accordance with fundamental rights as general principles of Union law as well as international law, including refugee protection, the principle of non-refoulement and human rights obligations, and in compliance with the provisions of Directive 2008/115/EC[9], is an important part of the comprehensive efforts to address migration in a fair and efficient way and, in particular, to reduce and deter irregular migration. To increase the effectiveness of the Union system to return illegally staying third-country nationals or stateless persons is needed in order to maintain public trust in the Union migration and asylum system, and should go hand in hand with the efforts to protect those in need of protection.

(21) For that purpose, it ***is*** also necessary to clearly ***record*** in Eurodac the fact that an application for international protection has been rejected where the third-country national or stateless person has no right to remain and has not been allowed to remain in accordance with Regulation (EU) …/… [Asylum Procedure Regulation].

[9] Directive 2008/115/EC 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).

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

(23) With a view to facilitating the procedures for the identification and the issuance of travel documents for return purposes of illegally staying third-country nationals or stateless persons, a scanned colour copy of an identity or travel document should be recorded in ***Eurodac*** where available, along with an indication of its authenticity. If such identity or travel document is not available, only one other available document identifying the third-country national or stateless person should be recorded in ***Eurodac*** along with an indication of its authenticity. In order to facilitate the procedures for the identification and the issuance of travel documents for return purposes of illegally staying third-country nationals or stateless persons, and in order not to populate the system with counterfeit documents, only documents validated as authentic or whose authenticity cannot be established due to the absence of security features, should be kept in the system.

(24) 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[10]. Member States should have the necessary tools at their disposal to be able to control illegal migration to the Union and to detect secondary movements and illegally staying third-country nationals and stateless persons in the Union. Therefore, the data in Eurodac should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of the Member States.

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

(25) The European Border and Coast Guard Agency, as established by Regulation (EU) 2016/1624 of the European Parliament and of the Council[11], supports Member States in their efforts to better manage the external borders and control illegal immigration. The European Union Agency for Asylum as established by [Regulation on the EU Agency for Asylum] provides operational and technical assistance to Member States. Consequently, authorised users of these agencies as well as of other Justice and Home Affairs Agencies should be provided with access to the central repository if such access is relevant for the implementation of their tasks in line with relevant data protection safeguards.

(26) As members of the European Border and Coast Guard Teams and experts of the asylum support teams referred to in Regulation (EU) 2016/1624 and Regulation (EU) ***2021/2303***[12] respectively may, upon request of the host Member State, take and transmit biometric data, adequate technological solutions should be developed to ensure that efficient and effective assistance is provided to the host Member State.

---

[11] ***Regulation (EU) 2016/1624 of the European Parliament and the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).***

[12] ***Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010 (OJ L 468, 30.12.2021, p. 1).***

(27) Moreover, in order for Eurodac to effectively assist with the control of irregular ***immigration to the Union,*** and with the detection of secondary movements within the ***Union*** it is necessary to allow the system to count applicants in addition to applications by linking all sets of data corresponding to one person, regardless of their category, in one sequence. ***Where a dataset registered in Eurodac is erased, any link to that dataset is to be automatically erased.***

(28) 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 Directive (EU) 2017/541 ***of the European Parliament and of the Council***[13] or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA[14]. 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). ▌ 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.

---

13 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

14 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).

(29) 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.

(30) The Commission outlined in its Communication to the Council and the European Parliament of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs that authorities responsible for internal security could have access to Eurodac in well-defined cases, when there is a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for international protection. In that Communication the Commission also found that the proportionality principle requires that Eurodac be queried for such purposes only if there is an overriding public security concern, that is, if the act committed by the criminal or terrorist to be identified is so reprehensible that it justifies querying a database that registers persons with a clean criminal record, and it concluded that the threshold for authorities responsible for internal security to query Eurodac must therefore always be significantly higher than the threshold for querying criminal databases.

(31) 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 Regulation (EU) 2016/794 ▌[15].

(32) Requests for comparison of Eurodac data by Europol should be allowed only in specific cases, under specific circumstances and under strict conditions, in line with the principles of necessity and proportionality enshrined in Article 52(1) of the Charter of Fundamental Rights of the European Union ***('the Charter')*** and as interpreted by the Court of Justice of the European Union[16].

---

[15] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

[16] Judgment of the Court of Justice of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238;Judgment of the Court of Justice of 21 December 2016, Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, Joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.

(33) 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 further development to the original purpose of Eurodac. In line with the requirements of Article 52(1) of the Charter ▌, any interference with the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary to genuinely meet an objective of general interest and proportionate to the legitimate objective it aims to achieve.

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

(35) This Regulation also lays down the conditions under which requests for comparison of biometric or alphanumeric data with Eurodac data for the purposes of preventing, detecting, or investigating terrorist offences or other serious criminal offences should be allowed and the necessary safeguards to ensure the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac. The strictness of those conditions reflects the fact that the Eurodac database registers biometric and alphanumeric data of persons who are not presumed to have committed a terrorist offence or other serious criminal offence. It is acknowledged that law enforcement authorities and Europol do not always have the biometric data of the suspect or victim whose case they are investigating, which may hamper their ability to check biometric matching databases such as Eurodac. It is important to equip law enforcement authorities and Europol with the necessary tools to prevent, detect and investigate terrorist offences or other serious criminal offences where it is necessary to do so. In order to contribute further to the investigations carried out by those authorities and Europol, searches based on alphanumeric data should be allowed in Eurodac, in particular in cases where no biometric evidence can be found, but where those authorities and Europol possess evidence of the personal details or identity documents of the suspect or victim.

(36) The ▌ expansion of the scope and simplification of law enforcement access to Eurodac should help Member States dealing with the increasingly complicated operational situations and cases involving cross-border crimes and terrorism with direct impact on the security situation in the EU. The conditions of access to Eurodac for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences should also allow the law enforcement authorities of the Member States to tackle the cases of suspects using multiple identities. For this purpose, obtaining a hit during a consultation of a relevant database prior to acceding Eurodac should not prevent such access. It may also be a useful tool to respond to the threat from radicalised persons or terrorists who might have been registered in Eurodac. A broader and simpler access of law enforcement authorities of the Member States to Eurodac should, while guaranteeing the full respect of the fundamental rights, enable Member States to use all existing tools to ensure an area of freedom, security and justice.

(37) 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 Regulation (EU) …/… [Qualification Regulation] of the European Parliament and of the Council, Regulation (EU) …/… establishing a [Union Resettlement Framework] and Regulation (EU) …/… [▌ Asylum and Migration Management], this Regulation includes in its scope applicants for subsidiary protection and persons eligible for subsidiary protection.

(38) It is ***also*** necessary to require the Member States promptly to take and transmit the biometric data of every applicant for international protection, of every person for whom Member States intend to conduct an admission procedure in accordance with Regulation (EU) …/… [Resettlement Regulation]**,** 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 ***and of every person disembarked following a search and rescue operation***, if they are at least six years of age.

▌

(39) The obligation to take the biometric data of illegally staying third country nationals or stateless persons of at least six years of age does not affect the Member States' right to extend a third-country national or stateless person's stay on their territory pursuant to Article 20(2) of the Convention implementing the Schengen Agreement.

(40) The fact that the application for international protection follows or is made simultaneously with the apprehension of the third-country national or stateless person in connection with the irregular crossing of the external borders does not exempt Member States from registering those persons as persons apprehended in connection with the irregular crossing of the external border.

(41) The fact that the application for international protection follows or is made simultaneously with the apprehension of the third-country national or stateless person illegally staying on the territory of Member States, does not exempt Member States from registering those persons as persons found to be illegally staying on the territory of the Member States.

(42) The fact that the application for international protection follows or is made simultaneously with the disembarkation following a search and rescue operation of the third-country national or stateless person does not exempt Member States from registering those persons as persons disembarked following a search and rescue operation.

(43) The fact that an application for international protection follows or is made simultaneously with the registration of the beneficiary of temporary protection does not exempt Member States from registering those persons as beneficiaries of temporary protection.

(44) In view of strengthening the protection of all children falling under the scope of this Regulation, including unaccompanied minors who have not applied for international protection and those children who may become separated from their families, it is also necessary to take biometric data for storage in the ***Eurodac*** to help establish the identity of children and assist a Member State in tracing any family or links they may have with another Member State, as well as in assisting a Member State in tracing missing children, including for law enforcement purposes, by complementing the existing instruments, in particular ▌ SIS ▌. Effective identification procedures will assist Member States in guaranteeing the adequate protection of children. Establishing family links is a key element in restoring family unity and must be closely linked to the determination of the best interests of the child and eventually, the determination of a sustainable solution in accordance with national practices following a needs assessment by the competent national child protection authorities.

(45) The official responsible for taking the biometric data of a minor should receive training so that sufficient care is taken to ensure an adequate quality of biometric data of the minor and to guarantee that the process is child-friendly so that the minor, particularly a very young minor, feels safe and can readily cooperate with the process for having his or her biometric data taken.

(46) Any minor from the age of six years old and above should be accompanied by, where present, an adult family member throughout the time his or her biometric data are taken. The unaccompanied minor should be accompanied by a ▌ representative or, where a representative has not been designated, a person trained to safeguard the best interests of the minor and his or her general wellbeing, throughout the time his or her biometric data are taken. Such a trained person should not be the official responsible for taking the biometric data, should act independently and should not receive orders either from the official or the service responsible for taking the biometric data. Such a trained person should be the person designated to provisionally act as a representative under Directive (EU) …/… [Reception Conditions Directive] where that person has been designated. The official responsible for taking the biometric data of a minor should also receive training so that sufficient care is taken to ensure an adequate quality of fingerprints of the minor and to guarantee that the process is child-friendly so that the minor, particularly a very young minor, feels safe and can readily cooperate with the process for having his or her biometric data taken.

(47) 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, those data may only be used for law enforcement purposes, in particular those relating to the prevention, detection and investigation of child trafficking and other serious crimes against children, by the requesting Member State and 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.

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

(49) Member States should ensure the transmission of biometric data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint and facial recognition system. All authorities with a right of access to Eurodac should invest in adequate training and in the necessary technological equipment. The authorities with a right of access to Eurodac should inform eu-LISA of specific difficulties encountered with regard to the quality of data, in order to resolve them.

(50) The fact that it is temporarily or permanently impossible to take and/or to transmit biometric data, due to reasons such as insufficient quality of the data for appropriate comparison, technical problems, reasons linked to the protection of health or due to the data subject being unfit or unable to have his or her biometric data taken owing to circumstances beyond his or her control, should not adversely affect the examination of or the decision on the application for international protection ▌ registered ▌ by that person.

(51) Member States should refer to the Commission Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints which the Council invited the Member States to follow on 20 July 2015[17]. It sets out a best practice approach to taking fingerprints. Where relevant, Member States should also take into account the Checklist to act in compliance with fundamental rights when obtaining fingerprints for Eurodac of the European Union Agency for Fundamental Rights which aims to assist them with complying with fundamental rights obligations when taking fingerprints.

[17] ***COM***(2015) 150 final, 27.5.2015

(52) Member States should inform all persons required by this Regulation to give biometric data of their obligation to do so. Member States should also explain to those persons that it is in their interests to fully and immediately cooperate with the procedure by providing their biometric data. Where a Member State's national law allows for the taking of biometric data by use of coercion as a last resort, those measures must fully respect the Charter ▌. Only in duly justified circumstances and as a last resort, having exhausted other possibilities, a proportionate degree of coercion could be used to ensure the compliance of third-country nationals or stateless persons who are deemed to be vulnerable persons, and minors, with the obligation to provide biometric data.

(53) Where detention is used in order to determine or verify a third-country national's or stateless person's identity, it should only be used by Member States as a means of last resort and in full respect of the Convention on Human Rights and Fundamental Freedoms, and in compliance with relevant Union law, including ***the*** Charter ▌.

(54) Where necessary, hits should be checked by a trained fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) …/… [▌ Asylum and Migration Management], 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. Check by a trained expert should be considered necessary where there is doubt that the result of the comparison of the fingerprint data relates to the same person, in particular where the data corresponding to a fingerprint hit belong to a person of different sex or where the facial image data do not correspond to the facial feature of the person whose biometric data were taken. Hits obtained from Eurodac based on facial images should also be checked by an expert trained in accordance with national practice, where the comparison is made with facial image data only. Where a fingerprint and facial image data comparison is carried out simultaneously and hits are returned for both biometric data sets, Member States should be able to check the result of the comparison of the facial image data.

(55) Third-country nationals or stateless persons who have requested international protection in one Member State may try to request international protection in another Member State for many years to come. The maximum period during which biometric data of third-country nationals or stateless persons who have requested international protection can be kept by the ***Eurodac*** should be limited to the extent strictly necessary and should be proportionate, in line with the principle of proportionality enshrined in Article 52(1) of the Charter and as interpreted by the Court of Justice. Given that most third-country nationals or stateless persons who have stayed in the Union for several years will have obtained a settled status or even citizenship of a Member State after that period, a period of ***10*** years should be considered a reasonable period for the storage of biometric and alphanumeric data.

▌

(56) ***In its conclusions on Statelessness of 4 December 2015, the Council and the Representatives of the Governments of the Member States recalled the Union's pledge of September 2012 that all Member States were to accede to the 1954 Convention relating to the Status of Stateless Persons and were to consider acceding to the 1961 Convention on the Reduction of Statelessness.***

(57) ***For the purposes of applying the refusal grounds under Regulation (EU) …/…*** [Resettlement Regulation]***, the biometric data of third-country nationals or stateless persons registered for the purpose of conducting an admission procedure under that Regulation should be taken, transmitted to Eurodac and compared against the data stored in Eurodac of beneficiaries of international protection, of persons who have been granted*** international protection or a ***national*** humanitarian status ***in accordance with Regulation (EU) …/… [Resettlement Regulation], who have been refused admission to a Member State on one of*** the ▌ grounds ***referred to in Article 6(1)(f) of*** Regulation (EU) …/… [Resettlement Regulation] ***or in respect of whom that procedure for admission has been discontinued, because they have not given or have withdrawn their consent and of persons who have been resettled under a national resettlement scheme. Therefore, those categories of data should be stored in Eurodac and made available for comparison***.

(58) For the purposes of applying Regulation (EU) …/… [Resettlement Regulation] and the [▌ Asylum and Migration Management ***Regulation***], the biometric data of third-country nationals or stateless persons ***granted international protection or a national humanitarian status in accordance with Regulation (EU) …/… [Resettlement Regulation*** should be stored in ***Eurodac*** for ***five*** years from the date on which they were taken. Such a period should be sufficient given the fact that the majority of such persons will have resided for several years in the Union and will have obtained a long-term resident status or even citizenship of a Member State.

(59) Where a third-country national or a stateless person has been refused admission to a Member State ***on one of the grounds referred to in Article 6(1)(f) of*** Regulation (EU) …/… [Resettlement Regulation], the related data should be stored for a period of three years from the date on which the negative conclusion on admission was reached. It is necessary to store such data for that length of time in order to allow other Member States conducting an admission procedure to receive information, including any information on the marking of data by other Member States, from ***Eurodac*** throughout the procedure to refuse admission, where necessary, by applying the refusal ***ground*** set out in ***Article 6(1)(f) of*** Regulation (EU) …/… [Resettlement Regulation]. In addition, data on admission procedures that have previously been discontinued because the third-country nationals or stateless persons have not given or have withdrawn their consent should be stored ***for three years*** in Eurodac in order to allow the other Member States conducting an admission procedure to ▌ reach a negative conclusion, ***as*** permitted by Regulation (EU) …/… [Resettlement Regulation].

(60) The ***transmission*** of ▌ data of persons registered for the purpose of conducting an admission procedure in ***Eurodac*** should ***contribute to limiting*** the number of Member States that exchange those persons' personal data within a subsequent admission procedure and thus it should contribute to ensuring compliance with the principle of data minimisation.

(61) Where a hit is received by a Member State from Eurodac that can assist that Member State in carrying out its obligations necessary for the application of grounds for refusing admission under the [Resettlement Regulation], the Member State of origin of the data which had previously refused to admit a third-country national or a stateless person should promptly exchange supplementary information with the Member State that received the hit in accordance with the principle of sincere cooperation and subject to the principles of data protection. Such exchange of data should allow the Member State that received the hit to reach a conclusion on the admission within the time limit set in [Resettlement Regulation] for concluding the admission procedure.

(62) The obligation to collect and transmit the biometric data of persons registered for the purpose of conducting an admission procedure should not apply where the Member State in question discontinues the procedure before the biometric data were taken.

(63) 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[18] and the right to protection of personal data, a period of five years should be considered a necessary period for the storage of biometric and alphanumeric data.

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

(64) In order to support the Member States in their administrative cooperation during the implementation of Council Directive 2001/55/EC data of beneficiaries of temporary protection should be kept in the Eurodac for a period of one year from the date of the entry into force of the relevant Council Implementing Decision. The retention period should be extended yearly for the duration of the temporary protection.

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

(66) It is appropriate to store data relating to those data subjects whose biometric data were initially recorded in Eurodac upon ▌ registering ***or making*** their applications for international protection ▌ and who have been granted international protection in a Member State in order to allow data recorded upon ▌ registering ***or making their*** application for international protection ▌ to be compared against them.

(67) Eu-LISA has been entrusted with the Commission's tasks relating to the operational management of Eurodac in accordance with this Regulation and with certain tasks relating to the Communication Infrastructure as from the date on which eu-LISA took up its responsibilities on 1 December 2012. In addition, Europol should have observer status at the meetings of the Management Board of eu-LISA when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by Europol for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of eu-LISA.

(68) It is necessary to lay down clearly the respective responsibilities of the Commission and eu-LISA, in respect of ***Eurodac*** and the Communication Infrastructure, and of the Member States, as regards data processing, data security, access to, and rectification of recorded data.

(69) 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.

(70) It is necessary to designate and keep a list of the operating unit(s) of Europol that are authorised to request comparisons with Eurodac data through the Europol Access Point. Such units, including units dealing with trafficking in human beings, sexual abuse and sexual exploitation, in particular where victims are minors, should be authorised to request comparisons with Eurodac data through the Europol Access Point in order 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.

(71) Requests for comparison with data stored in ***Eurodac*** 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 ***Eurodac*** 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.

(72) 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.

(73) 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.

(74) In addition, access should be allowed ▌ on condition that a prior search in the national biometric databases of the Member State and in the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA[19] has been conducted***, unless the consultation of CIR in accordance with Article 22(2) of Regulation (EU) 2019/818 indicates that the data ot the person concerned is stored in Eurodac***. 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. In addition to the prior check of the databases, designated authorities should also be able to conduct a simultaneous check in the Visa Information System, provided that the conditions for a comparison with the data stored therein, as laid down in Decision 2008/633/JHA, are met.

▌

[19] 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*)*.

(75) 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.

(76) 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.

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

(78) Regulation (EU) 2016/679 of the European Parliament and of the Council▌ applies to the processing of personal data by the Member States carried out in application of this Regulation unless such processing is carried out by the designated or verifying competent authorities of the Member States for the purposes of the prevention, investigation, detection or prosecution of terrorist offences or of other serious criminal offences including the safeguarding against and the prevention of threats to public security.

(79) The national provisions adopted pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data▌ apply to the processing of personal data by competent authorities of the Member States for the purposes of the prevention, investigation, detection or prosecution of terrorist offences or of other serious criminal offences pursuant to this Regulation.

(80) Regulation (EU) 2016/794 applies to the processing of personal data by Europol for the purposes of the prevention, investigation or detection of terrorist offences or of other serious criminal offences pursuant to this Regulation.

(81) The rules set out in Regulation (EU) 2016/679 regarding the protection of the rights and freedoms of individuals, notably their right to the protection of personal data concerning them, with regard to the processing of personal data should be specified in respect of the responsibility for the processing of the data, of safeguarding the rights of data subjects and of the supervision of data protection, in particular as far as certain sectors are concerned.

(82) A person's right to privacy and to data protection should be safeguarded in accordance with this Regulation at all times, both with regard to access by the Member States' authorities and by the European Union's authorised agencies.

(83) Data subjects should have the right of access to, rectification and erasure of personal data concerning them and of restriction of the processing thereof. Taking into account the purposes for which the data are processed, data subjects should have the right to completion of incomplete personal data, including by means of providing a supplementary statement. Those rights should be exercised pursuant to Regulation (EU) 2016/679 and in accordance with the procedures set out in this Regulation, Directive (EU) 2016/680 and Regulation (EU) 2016/794 as regards the processing of personal data for law enforcement purposes pursuant to this Regulation. In relation to the processing of personal data in Eurodac by national authorities, each Member State, for reasons of legal certainty and transparency, should designate the authority which is to be considered as controller in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680 and which should have central responsibility for the processing of data by that Member State. Each Member State should communicate the details of that authority to the Commission.

(84) It is also important that factually incorrect data recorded in Eurodac are rectified, in order to ensure that statistics produced in accordance with this regulation are accurate.

(85) Transfers of personal data obtained by a Member State or Europol pursuant to this Regulation from ***Eurodac*** 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 ***persons whose data are processed*** under ***this*** Regulation ▌ from having their data disclosed to a third country. This implies that Member States should not transfer information obtained from ***Eurodac*** concerning: the name(s); date of birth; nationality; the Member State(s) of origin or Member State of relocation or the Member State of resettlement; the details of the identity or travel document; the place and date of resettlement or of the application for international protection; the reference number used by the Member State of origin; the date on which the biometric data were taken as well as the date on which the Member State(s) transmitted the data to Eurodac; the operator user ID; and any information relating to any transfer of the data subject under Regulation (EU) …/… [▌ Asylum and Migration Management]. That prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) …/… [▌ Asylum and Migration Management] applies ▌ in accordance with Regulation (EU) 2016/679 and with the national rules adopted pursuant to Directive (EU) 2016/680, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

(86) As a derogation to the rule that no personal data obtained by a Member State pursuant to this Regulation should be transferred or made available to any third country, it should be possible to transfer such personal data to a third country where such a transfer is subject to strict conditions and is necessary in individual cases in order to assist with the identification of a third-country national in relation to his or her return. Sharing of any personal data should be subject to strict conditions. Where such information is shared, no information should be disclosed to a third-country relating to the fact that an application for international protection has been made by that third-country national. The transfer of any personal data to third countries should be carried out in accordance with the provisions of Regulation (EU) 2016/679 and be conducted with the agreement of the Member State of origin. The third countries of return are often not subject to adequacy decisions adopted by the Commission under Article 45 of Regulation (EU) 2016/679. Furthermore, the extensive efforts of the Union in cooperating with the main countries of origin of illegally staying third-country nationals subject to an obligation to return has not been able to ensure the systematic fulfilment by such third countries of the obligation established by international law to readmit their own nationals. Readmission agreements, concluded or being negotiated by the Union or the Member States and providing for appropriate safeguards for the transfer of data to third countries pursuant to Article 46 of Regulation (EU) 2016/679 cover a limited number of such third countries and conclusion of any new agreement remains uncertain. In such situations, and as an exception to the requirement of an adequacy decision or appropriate safeguards, transfer of personal data to third-country authorities pursuant to this Regulation should be allowed for the purposes of implementing the return policy of the Union, and it should be possible to use the derogation provided for in Article 49 of Regulation (EU) 2016/679, provided that the conditions laid down in that Regulation are met. According to its Article 57, implementation of Regulation (EU) 2016/679 ▌, including with regard to transfers of personal data to third countries pursuant to this Regulation, is subject to monitoring by the national independent supervisory authority. Regulation (EU) 2016/679 applies regarding the responsibility of the Member States' authorities as ‘controllers’ within the meaning of that Regulation.

▌

(87) Regulation (EU) 2018/1725[20], and in particular Article 33 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, without prejudice to Regulation (EU) 2016/794, which should apply to the processing of personal data by Europol. 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) …/… [▌ Asylum and Migration Management ***Regulation***] and Regulation (EU) …/… [Resettlement Regulation].

(88) 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) …/… [▌ Asylum and Migration Management ***Regulation***] and Regulation (EU) …/… [Resettlement Regulation], and of the use to which law enforcement authorities may put his or her data.

[20] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(89) It is appropriate that national supervisory authorities established in accordance with Regulation (EU) 2016/679 monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor, as established in ▌Regulation (***EU***) ***2018/1725 of the European Parliament and of the Council***[21], 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. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the processing of personal data***, including in the context of the Coordinated Supervision Committee established within the framework of the European Data Protection Board***.

(90) The European Data Protection Supervisor was consulted in accordance with Article 42 of Regulation (EU) 2018/1725 and delivered ***an opinion*** on 21 September 2016 and ***on 30 November 2020.***

(91) 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.

---

[21] ***Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).***

(92) It is appropriate to monitor and evaluate the performance of Eurodac at regular intervals, including in terms of whether law enforcement access has led to indirect discrimination against applicants for international protection, as raised in the Commission's evaluation of the compliance of this Regulation with the Charter ▌. Eu-LISA should submit an annual report on the activities of ***Eurodac*** to the European Parliament and to the Council.

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

(94) 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) …/… [▌ Asylum and Migration Management ***Regulation***].

(95) This Regulation should be without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council[22].

(96) 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.

---

[22] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

(97) 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.

▌

(98) 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.

▌

(99) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of Regulation (EU) …/… [Asylum and Migration Management Regulation], with the exception of the provisions related to data collected to assist with the application of Regulation (EU) …/… [Resettlement Regulation] under the conditions set out in this Regulation,

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) ***support the asylum system, including by assisting*** in determining which Member State is to be responsible pursuant to Regulation (EU) …/… [Regulation on Asylum and Migration Management] for examining an application for international protection registered in a Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] under the conditions set out in this Regulation;

(b) assist with the application of Regulation (EU) …/… [Resettlement Regulation] under the conditions set out in this Regulation;

(c) assist with the control of irregular immigration to the Union and with the detection of secondary movements within the Union and with the identification of illegally staying third-country nationals and stateless persons for determining the appropriate measures to be taken by Member States;

(d) ***assist with the protection of children, including in the context of law enforcement***;

(e) lay down the conditions under which Member States' designated authorities and the European ***Union Agency for Law Enforcement Cooperation*** (Europol) may request the comparison of biometric or alphanumeric data with those stored in ***Eurodac*** for law enforcement purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences;

(f) assist in the correct identification of persons registered in Eurodac under the conditions and for the ▌ objectives referred to in Article 20 of Regulation (EU) 2019/818 by storing identity data, travel document data and biometric data in the ▌ CIR ▌ established by ▌ that Regulation;

(g) support the objectives of the European Travel Information and Authorisation System (‘ETIAS’) established by Regulation (EU) 2018/1240▌;

(h) support the objectives of the Visa Information System (VIS) ***referred to in*** Regulation (EC) No 767/2008▌***;***

(i) ***support evidence-based policy making through the production of statistics;***

(j) ***assist with the implementation of the Directive 2001/55/EC***.

2. Without prejudice to the processing of data intended for Eurodac by the Member State of origin in databases set up under the latter's national law, biometric data and other personal data may be processed in Eurodac only for the purposes set out in this Regulation***,*** in Regulation (EU) …/… [Regulation on Asylum and Migration Management]***, in Regulation (EU) 2019/818, in Regulation (EU) 2018/1240, in Regulation (EC) No 767/2008,*** in Regulation (EU) …/… [Resettlement Regulation] ***and in Directive 2001/55/EC [Temporary Protection Directive]***

This Regulation fully respects human dignity and the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, including the right to respect for one's private life, the right to the protection of personal data, the right to asylum and the prohibition of torture and inhuman or degrading treatment. In that respect, the processing of personal data in accordance with this Regulation shall not result in any discrimination against persons covered by this Regulation based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

A person's right to privacy and to data protection shall be safeguarded in accordance with this Regulation at all times, both with regard to access by the Member States' authorities and by the European Union's authorised agencies.

Article 2

Obligation to take biometric data

1. Member States are obliged to take the biometric data of persons referred to in Article 15(1), 18, 20, 22(1)***,*** 23(1)***, 24(1) and 26(1)*** for the purposes of Article 1(1)(a), ▌(b)***,*** (c) ***and (j)*** of this Regulation and shall impose on those persons the requirement to provide their biometric data and inform them in accordance with Article 42 of this Regulation.

2. Member States shall, at all times, respect the dignity and physical integrity of the person during the fingerprinting procedure and when capturing his or her facial image.

3. Administrative measures for the purpose of ensuring compliance with the obligation to provide biometric data ▌in accordance with paragraph 1 of this Article shall be laid down in national law. These measures shall be effective, proportionate and dissuasive and may include the possibility to use means of coercion as a last resort.

4. Where all of the measures laid down in national law in accordance with paragraph 3 fail to ensure the compliance by an applicant with the obligation to provide biometric data, the relevant provisions of Union law on asylum concerning the non-compliance with that obligation shall apply.

▌

5. Without prejudice to paragraphs 3 and 4 of this Article, where it is impossible to take the biometric data of a third-country national or stateless person who is deemed to be a vulnerable person, due to the condition of that person's fingertips or face, and where that person did not intentionally bring about the condition, the authorities of that Member State shall not employ administrative measures for ensuring compliance with the obligation to provide biometric data.

6. The procedure for taking biometric data shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms.

Article 3

Special provisions relating to minors

1. The biometric data of minors from the age of six shall be taken by officials trained specifically to take a minor's biometric data in a child-friendly and child-sensitive manner and in full respect of the best interests of the child and the safeguards laid down in the United Nations Convention on the Rights of the Child.

The best interests of the child shall be a primary consideration in the application of this Regulation. In the event that there is uncertainty as to whether or not a child is under the age of 6 years and there is no supporting proof of age, then the competent authorities of the Member States shall consider that child to be under the age of 6 years for the purposes of this Regulation.

The minor shall be accompanied by, where present, an adult family member throughout the time his or her biometric data are taken. The unaccompanied minor shall be accompanied by a representative or, where a representative has not been designated, a person trained to safeguard the best interests of the minor and his or her general wellbeing, throughout the time his or her biometric data are taken. Such a trained person shall not be the official responsible for taking the biometric data, shall act independently and shall not receive orders either from the official or the service responsible for taking the biometric data. Such a trained person shall be the person designated to provisionally act as a representative under Directive (EU) …/… [Reception Conditions Directive] where that person has been designated.

No form of force shall ▌ be used against minors to ensure their compliance with the obligation to provide biometric data. However, where permitted by relevant Union or national law, and as a last resort a proportionate degree of coercion may be used against minors to ensure their compliance with that obligation. When applying such a proportionate degree of coercion, Member States shall respect the dignity and physical integrity of the minor.

2. Where the enrolment of the fingerprints or capturing the facial image of a minor is not possible due to the conditions of the fingertips or face, Article ***2(5***) shall apply. Where the fingerprints or facial image of a minor are retaken, the Member State concerned shall proceed in accordance with paragraph 1 of this Article. Where a minor, in particular an unaccompanied or separated minor, refuses to give their biometric data and there are reasonable grounds for believing that there are child safeguarding or protection risks, as assessed by an official trained specifically to take a minor's biometric data, the minor shall be referred to the competent national child protection authorities, the national referral mechanisms or both.

The provisions in this Regulation shall be without prejudice to the application of the conditions set out in Article 13 of Directive (EU) …/… [Reception Conditions Directive].

3. Eurodac data that pertain to a child under the age of fourteen shall only be used for law enforcement purposes against such a child when there are grounds in addition to those referred to in Article 33(1)(c) to consider that those data are necessary for the purposes of the prevention, detection or investigation of a terrorist offence or of another serious criminal offence which that child is suspected of having committed.

Article 4

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 ***3(7***) of Regulation (EU) …/… [Qualification Regulation] in respect of which a final decision has not yet been taken;

(b) ***a*** 'person registered for the purpose of conducting an admission procedure' means a person who has been registered for the purpose of conducting a resettlement or humanitarian admission procedure in accordance with Article ***9(3***) of Regulation (EU) …/… [Resettlement Regulation];

(c) ***a*** ‘person admitted in accordance with a national resettlement scheme’ means a person resettled by a Member State outside the framework of Regulation (EU) …/… [Resettlement Regulation]***, if that person is*** granted international protection as defined in Article ***3(3)*** of Regulation (EU) …/… [Qualification Regulation] or a humanitarian status under national law ***as defined in Article 2(2)(c) of Regulation (EU) …/… [Resettlement Regulation]*** in accordance with the rules governing the national resettlement scheme;

(d) ‘humanitarian status under national law’ means a humanitarian status under national law that provides for rights and obligations equivalent to the rights and obligations set out in Articles ***20*** to ***26*** and ***28*** to ***35*** of Regulation (EU) …/… [Qualification Regulation];

(e) ’Member State of origin’ means:

(i) in relation to a person covered by Article 15(1), the Member State which transmits the personal data to ***Eurodac*** and receives the results of the comparison;

(ii) in relation to a person covered by Article 18(1), the Member State which transmits the personal data to Eurodac and receives the results of the comparison;

(iii) in relation to a person covered by Article 18(2), the Member State which transmits the personal data to Eurodac;

(iv) in relation to a person covered by Article 20, the Member State which transmits the personal data to Eurodac;

(v) in relation to a person covered by Article 22(1), the Member State which transmits the personal data to ***Eurodac*** and receives the results of the comparison;

(vi) in relation to a person covered by Article 23(1), the Member State which transmits the personal data to ***Eurodac*** and receives the results of the comparison;

(vii) in relation to a person covered by Article 24(1), the Member State which transmits the personal data to ***Eurodac*** and receives the results of the comparison;

▌

(viii) in relation to a person covered by Article 26(1), the Member State which transmits the personal data to ***Eurodac*** and receives the results of the comparison**.**

(f) ‘third-country national’ means any person who is not a citizen of the Union within the meaning of Article 32(1) of the Treaty and who is not a national of a State which ***participates*** in this Regulation by virtue of an agreement with the Union;

(g) ‘illegal stay’ means the presence on the territory of a Member State, of a third-country national or a stateless person who does not fulfil, or no longer fulfils the conditions of entry as set out in Article ***6*** of ***the Schengen Borders Code*** or other conditions for entry, stay or residence in that Member State;

(h) ‘beneficiary of international protection’ ***means a*** means a person who has been granted refugee status ***as defined in Article 3(1) of Regulation (EU) …/… [Qualification Regulation]*** or subsidiary protection status as defined in Article ***3(2***) of Regulation (EU) …/… [Qualification Regulation];

(i) ‘beneficiary of temporary protection’ means a person who enjoys temporary protection as defined in Article 2(a) of Directive 2001/55/EC and in the Council Implementing Decision introducing temporary protection, or any other equivalent national protection introduced in response to the same event as that Council Implementing Decision;

(j) ‘hit’ means the existence of a match or matches established by ***Eurodac*** by comparison between biometric data recorded in the computerised central database and those transmitted by a Member State with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 38(4);

(k) ‘National Access Point’ means the designated national system which communicates with ***Eurodac***;

(l) ‘Europol Access Point’ means the designated Europol system which communicates with ***Eurodac***;

(m) ‘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) 2018/1726;

(n) ‘Europol’ means the European Police Office established by Regulation (EU) 2016/794;

(o) ‘Eurodac data’ means all data stored in ***Eurodac*** in accordance with ***Article 17***, ***Article*** 19 ▌, 21 ▌, ***Article*** 22(2), ***Article 23***(2)***, Article*** 24***(2) and 26***(2);

(p) ‘law enforcement’ means the prevention, detection or investigation of terrorist offences or of other serious criminal offences;

(q) ‘terrorist offences’ means the offences under national law which correspond or are equivalent to the offences referred to in Directive (EU) 2017/541;

(r) ‘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;

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

(t) ‘facial image data’ means digital images of the face with sufficient image resolution and quality to be used in automatic biometric matching;

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

(v) ‘alphanumeric data’ means data represented by letters, digits, special characters, space and punctuation marks;

(w) ‘residence document’ means any authorisation issued by the authorities of a Member State authorising a third-country national or a stateless person to stay on its territory, including the documents substantiating the authorisation to remain on the territory under temporary protection arrangements or until the circumstances preventing a removal order from being carried out no longer apply, with the exception of visas and residence authorisations issued during the period required to determine the Member State responsible as established in Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] or during the examination of an application for international protection or an application for a residence permit;

(x) ‘interface control document’ means a technical document that specifies the necessary requirements with which the National access points or the Europol access point are to comply in order to be able to communicate electronically with ***Eurodac***, in particular by detailing the format and possible content of the information to be exchanged between ***Eurodac*** and the National or the Europol access points***;***

(y) ‘CIR’ means the common identity repository as defined in Article 17***(1) and (2)*** of Regulation (EU) 2019/818;

(z) ‘identity data’ means the data referred to in Article 17(1)(c) to (f) and (h), Article 19(1)(c) to (f) and (h), Article 21(1)(c) to (f) and (h), Article 22(2)(c) to (f) and (h), Article 23(2)(c) to (f) and (h) ▌**,** Article 24(2)***(c) to (f) and (h), and Article 26(2)***(c) to (f) and (h);

(aa) ‘dataset’ means the set of information recorded in Eurodac on the basis of Articles 17, 19, 21, 22, 23***, 24*** or 26, corresponding to one set of fingerprints of a data subject and composed of biometric data, alphanumeric data and, where available, a scanned colour copy of an identity or travel document;

(ab) ‘child’ and ‘minor’ mean a person below the age of 18 years.

2. The terms defined in Article 4 of Regulation (EU) 2016/679 shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of the Member States for the purposes laid down in Article 1(1)(a) of this Regulation.

3. Unless stated otherwise, the terms defined in Article 2 of Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] shall have the same meaning in this Regulation.

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

Article 5

System architecture and basic principles

1. Eurodac shall consist of:

(a) a Central System composed of:

(i) a Central Unit,

(ii) a Business Continuity Plan and System;

(b) a communication infrastructure between the Central System and Member States that provides a secure and encrypted communication channel for Eurodac data ('Communication Infrastructure');

(c) the ▌ CIR ▌ as referred to in Article 4***(1)***(y) ▌ ;

(d) a secure communication infrastructure between the Central System and the central infrastructures of the European search portal ***and*** the CIR ▌ established by Regulation (EU) 2019/818.

2. The CIR shall contain the data referred to in Article 17***(1)***(a) to (f) ***and*** (h) and (i), Article 19(1)(a) to (f), (h) and (i), Article 21(1)(a) to (f), (h) and (i), Article 22(2)(a) to (f), (h) and (i), Article 23(2)(a) to (f), (h) and (i), Article 24(2)***(a) to (f) and (h) and (3)(a), and Article 26(2)***(a) to (f), (h) ▌ and (i). The remaining Eurodac data shall be stored in the Central System.

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

4. Each Member State shall have a single National Access Point. Europol shall have a single Europol access point.

5. Data on persons covered by Articles 15(1), 18***(2),*** 20, 22(1), 23(1), 24***(1)*** and 26(1) which are processed in ***Eurodac*** 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.

6. All ***datasets*** registered in Eurodac corresponding to the same third country national or stateless person shall be linked in a sequence. Where ***an automatic comparison is carried out in accordance with Articles 27 and 28*** and a hit is obtained against at least one other set of fingerprints***, or, where the latter are of a quality not ensuring appropriate comparison or are not available, facial image data,*** in another dataset corresponding to that same third country national or stateless person, Eurodac shall automatically link those datasets on the basis of the ▌ comparison. ***Where*** necessary, ***an*** expert ***shall check,*** in accordance with Article 38***(4) and (5), the result of an automatic comparison carried out in accordance with Articles 27 and 28***. When the receiving Member State confirms the hit, it shall send a notification to eu-LISA that will confirm the linking.

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

Article 6

Operational management

1. eu-LISA shall be responsible for the operational management of Eurodac.

The operational management of Eurodac shall consist of all the tasks necessary to keep Eurodac functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of ***Eurodac***. 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.

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 ***Eurodac***.

2. ***eu***-LISA shall be permitted to use real personal data of the Eurodac production system for testing purposes, in accordance with Regulation (EU) 2016/679, in the following circumstances:

(a) for diagnostics and repair when faults are discovered with ***Eurodac***; and

(b) for testing new technologies and techniques relevant to enhance the performance of ***Eurodac*** 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. Processing of real personal data adapted for testing shall be subject to stringent conditions and rendered anonymous in such a way that the data-subject is no longer identifiable. Once the purpose for which the testing was carried out has been achieved or the tests have been completed, such real personal data shall be immediately and permanently erased from the testing environment.

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

(a) supervision;

(b) security;

(c) the coordination of relations between the Member States and the provider.

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

(a) the implementation of the budget;

(b) acquisition and renewal;

(c) contractual matters.

5. Without prejudice to Article 17 of the Staff Regulations, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with Eurodac data. This obligation shall also apply after such staff leave office or employment or after the termination of their duties.

Article 7

Member States' designated authorities for law enforcement purposes

1. For the purposes laid down in Article 1(1)(e), Member States shall designate the authorities that are authorised to request comparisons with Eurodac data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

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

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

Article 8

Member States' verifying authorities for law enforcement purposes

1. For the purposes laid down in Article 1(1)(e), 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 7(3) and shall not receive instructions from them as regards the outcome of the verification.

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

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

   Only duly empowered staff of the verifying authority shall be authorised to receive and transmit a request for access to Eurodac in accordance with Article 32.

Only the verifying authority shall be authorised to forward requests for comparison of biometric or alphanumeric data to the National Access Point.

Article 9

Europol

1. For the purposes laid down in Article 1(1)(e), Europol shall designate one or more of its operating units as the 'Europol designated authority' that are authorised to request comparisons with Eurodac data through the Europol Access Point in order 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.

2. For the purposes laid down in Article 1(1)(e), Europol shall designate a single specialised unit with duly empowered Europol officials to act as its verifying authority which shall be authorised to forward requests by operating units for comparisons with Eurodac data through the Europol Access Point. The verifying authority shall be fully independent of the designated authority referred to in paragraph 1 of this Article when performing its tasks under this Regulation. The verifying authority shall be separate from the designated authority referred to in paragraph 1 and shall not receive instructions from it as regards the outcome of the verification. The verifying authority shall ensure that the conditions for requesting comparisons of biometric or alphanumeric data with Eurodac data are fulfilled.

Article 10

Interoperability with ETIAS

1. From … [the date of application of this ***Regulation],*** Eurodac shall be connected to the European search portal referred to in Article 6 of Regulation (EU) 2019/818 ***in order*** to enable the ***application of Articles*** 11 ***and 20*** of Regulation (EU) 2018/1240.

2. The automated processing referred to in Article ***20*** of Regulation (EU) 2018/1240 shall enable the verifications provided for in ***that*** Article ▌ and the subsequent verifications ***provided for in*** Articles 22 and 26 of that Regulation.

   For the purpose of carrying out the verifications referred to in Article 20(2)(k) of Regulation (EU) 2018/1240, the ETIAS Central System shall use the European search portal***,*** to compare the data in ETIAS with the data in Eurodac collected on the basis of Articles ***17,*** 19***, 21***, 22, 23***, 24*** and 26 ***of this Regulation in a read-only format using the data categories listed in Annex I*** of this Regulation corresponding to individuals having left or having been removed from the territory of the Member States in compliance with a return decision or removal order ▌ .

   The verifications shall be without prejudice to the specific rules provided for in Article 24(3) of Regulation (EU) 2018/1240.

Article 11

Conditions for access to Eurodac for the manual processing by ETIAS National Units

1. Consultation of Eurodac by ETIAS National Units shall ***be*** carried out by means of the same alphanumerical data as those used for the automated processing referred to in Article 10.

2. For the purposes of Article 1(1)(g) ▌ the ETIAS National Units ▌ shall have access to ▌ consult the Eurodac ***in accordance with Regulation (EU) 2018/1240***, in a read-only format, for the purpose of examining applications for travel authorisation. In particular, the ETIAS National Units may consult the data referred to in Articles 17, 19***, 21, 22***, 23***, 24*** and 26.

3. Following consultation and access pursuant to paragraphs 1 and 2 of this Article the result of the assessment shall be recorded only in the ETIAS application files.

Article 12

Access to Eurodac by the competent visa authorities

For the purpose of manually verifying hits triggered by the automated queries carried out by the Visa Information System in accordance with Articles 9a and 9c of Regulation (EC) No 767/2008 and examining and deciding on visa applications in accordance with Article 21 of Regulation (EC) No 810/2009 of the European Parliament and of the Council[23], the competent visa authorities shall***, in accordance with those Regulations,*** have access to Eurodac to consult data in a read-only format.

Article 13

Interoperability with ***the Visa Information System***

From the … [date of application of the Regulation (EU) …/… amending the VIS Regulation], as provided for in Article 9 of that Regulation, Eurodac shall be connected to the European search portal referred to in Article 6 of Regulation (EU) 2019/817 in order to enable the automated processing referred to in Article 9a of Regulation (EC) No 767/2008 ***and therefore*** to query Eurodac and compare the relevant data in the Visa Information System with the relevant data in Eurodac. The verifications shall be without prejudice to the specific rules provided for in Article 9(b) of Regulation (EC) No 767/2008. ▌

[23] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

Article 14

Statistics

1. eu-LISA shall draw up statistics on the work of ***Eurodac*** every month indicating in particular:

(a) the number of applicants and the number of first-time applicants ***resulting*** from the linking process referred to in Article 5(6);

(b) the number of rejected applicants resulting from the linking process ***referred to in Article 5(6) and pursuant to Article 17(2)(j);***

(c) the number of persons disembarked following search and rescue operations;

(d) the number of persons registered as beneficiaries of temporary protection;

(e) the number of applicants who have been granted international protection in a Member State;

(f) the number of persons who were registered as minors;

(g) the number of persons referred to in Article 18***(2)(a) who were resettled under Regulation (EU) …/… [Resettlement Regulation];***

(h) ***the number of persons referred*** to ***in*** Article 20 ***who were resettled under a national resettlement scheme***;

(i) the number of data sets transmitted ***on persons referred to in Articles 15***(1), 18***(2)(b)***, 18***(2)(c)***, 22(1), 23(1), ***24(1)*** and 26***(1);***

(j) ***the number of transmissions of data on persons referred to in Articles 12a(1)***;

(k) the number of hits for persons referred to in Article 15(1):

(i) for whom an application for international protection was registered ▌ in a Member State;

(ii) who were apprehended in connection with the irregular crossing of an external border;

(iii) who were illegally staying in a Member State;

(***iv)*** ***who were disembarked following a search and rescue operation;***

(v) ***who have been granted international protection in a Member State;***

(vi) ***who were registered as a beneficiary of temporary protection in a Member State;***

(vii) who have been registered for the purpose of conducting an admission procedure ▌ in accordance with Regulation (EU) …/… [Resettlement Regulation] ▌ and

- ***have been granted international protection or a national humanitarian status in accordance with Regulation (EU) …/… [Resettlement Regulation];***

- ***have been refused admission on one of the grounds referred to in Article 6(1)(f) of Regulation (EU) …/… [Resettlement Regulation]; or***

- ***for whom the admission procedure has been discontinued due to the fact that that person did not give or withdrew his or her consent in accordance with Article 7 of Regulation (EU) …/… [Resettlement Regulation];***

(viii) who ***have been*** admitted in accordance with a national resettlement scheme**.**

▌

(l) the number of hits for persons referred to in Article 18(1):

(i) who have previously been granted international protection in a Member State,

(ii) who have been registered for the purpose of conducting an admission procedure in accordance with Regulation (EU) …/… [Resettlement Regulation] and:

- ***have been granted international protection or a humanitarian status under national law;***
- ***have been refused admission on one of the grounds referred to in Article 6(1)(f) of Regulation (EU) …/… [Resettlement Regulation]; or***
- ***for whom the admission procedure was discontinued due to the fact that that person did not give or withdrew his or her consent in accordance with Article 6a of Regulation (EU) …/… [Resettlement Regulation];***

(iii) who have been admitted in accordance with a national resettlement scheme.

(m) the number of hits for persons referred to in Article 22(1):

(i) for whom an application for international protection was registered ***in a Member State***,

(ii) who were apprehended in connection with the irregular crossing of an external border,

(iii) who were illegally staying in a Member State;

(iv***)*** ***who were disembarked following a search and rescue operation;***

(v) who have been granted international protection in a Member State;

(vi) who have been registered for the purpose of conducting an admission procedure in accordance with Regulation (EU) …/… [Resettlement Regulation] ***and:***

– ***have been granted international protection or a humanitarian status under national law;***

– ***have been refused admission on one of the grounds referred to in Article 6(1)(f) of Regulation (EU) …/… [Resettlement Regulation];***

– ***for whom the admission procedure was discontinued due to the fact that that person did not give or withdrew his or her consent in accordance with Article 7 of Regulation (EU) …/… [Resettlement Regulation];***

(vii) who ***have been*** admitted ▌ in accordance with a national resettlement scheme***;***

(viii) who were registered as a beneficiary of temporary protection in a Member State;

(n) the number of hits for persons referred to in Article 23(1):

(i) for whom an application for international protection ***was registered in a Member State;***

(ii) who were apprehended in connection with the irregular crossing of an external border***;***

(iii) who were illegally staying in a Member State;

▌

(***iv***) who were disembarked following a search and rescue operation;

(v***)*** ***who have been granted international protection in a Member State;***

(vi) who have been registered for the purpose of conducting an admission procedure in accordance with Regulation (EU) …/… [Resettlement Regulation] and:

- ***have been granted international protection or a humanitarian status under national law;***
- ***have been refused admission on one of the grounds referred to in Article 6(1)(f) of Regulation (EU) …/… [Resettlement Regulation];***
- ***for whom the admission procedure was discontinued due to the fact that that person did not give or withdrew his or her consent in accordance with Article 7 of Regulation (EU) …/… [Resettlement Regulation];***

(vii) who have been admitted in accordance with a national resettlement scheme***;***

(viii) who were registered as a beneficiary of temporary protection in a Member State;

(o) the number of hits for persons referred to in Article 24***(1)***:

(i) for ***whom*** an application for international protection ***was registered in a Member State***;

(ii) who were apprehended in connection with the irregular crossing of an external border;

(iii) who were illegally staying in a Member State;

(iv***)*** ***who were disembarked following a search and rescue operation;***

(v) who have been granted international protection in a Member State;

(vi) who have been registered for the purpose of conducting an admission procedure ▌ in accordance with Regulation (EU) …/… [Resettlement Regulation] ▌ and***:***

– ***have been granted international protection or a humanitarian status under national law;***

– ***have been refused admission on one of the grounds referred to in Article 6(1)(f) of Regulation (EU) …/… [Resettlement Regulation];***

– ***for whom the admission procedure was discontinued due to the fact that that person did not give or withdrew his or her consent in accordance with Article 7 of Regulation (EU) …/… [Resettlement Regulation];***

(vii) who ***have been*** admitted in accordance with a national resettlement scheme***;***

(viii) who were registered as a beneficiary of temporary protection in a Member State;

(p) the number of hits for persons referred to in Article 26(1):

(i) ***who have lodged*** an application for international protection ***in a Member State***,

(ii) who were apprehended in connection with the irregular crossing of an external border,

(iii) who were illegally staying in a Member State,

(iv***)*** ***who were disembarked following a search and rescue operation;***

(v) ***who have been granted international protection in a Member State;***

(vi) who have been registered for the purpose of conducting an admission procedure in accordance with Regulation (EU) …/… [Resettlement Regulation] ▌ and***:***

– ***have been granted international protection or a humanitarian status under national law;***

– ***have been refused admission on one of the grounds referred to in Article 6(1)(f) of Regulation (EU) …/… [Resettlement Regulation];***

– ***for whom the admission procedure was discontinued due to the fact that that person did not give or withdrew his or her consent in accordance with Article 7 of Regulation (EU) …/… [Resettlement Regulation];***

(vii) who ***have been*** admitted in accordance with a national resettlement scheme;

(viii) who were registered as beneficiary of temporary protection in a Member State;

(q) the number of biometric data which ***Eurodac*** had to request more than once from the Member States of origin because the biometric data originally transmitted did not lend themselves to comparison using the computerised fingerprint and facial image recognition systems;

(r) the number of data sets marked and unmarked in accordance with Article 31(1)**,** (2), (3) and (4);

(s) the number of hits for persons referred to in Article 31(1) and (4) for whom hits have been recorded under points (k) to (p) of this Article;

(t) the number of requests and hits referred to in Article 33(1);

(u) the number of requests and hits referred to in Article 34(1);

(v) the number of requests made ▌ in ***accordance with*** Article 43;

(w) the number of hits received from ***Eurodac*** as referred to in Article 38(6).

2. The monthly statistical data for persons referred to in paragraph 1(a) to (w) shall be published each month. At the end of each year, the yearly statistical data for persons referred to in paragraph 1(a) to (w) shall be published by eu-LISA. The statistical data shall ▌ be broken down by Member State. The statistical data for persons referred to in paragraph 1(i) shall, where possible, be broken down by year of birth and sex.

Nothing in this paragraph shall affect the anonymized nature of the statistical data.

3. For the purpose of supporting the objective referred to in Article 1(c) ***and (i)***, eu-LISA shall produce monthly cross-system statistics. Those statistics shall not allow for the identification of individuals and will use data from Eurodac, the Visa Information System, ETIAS***,*** and the ***EES***.

These statistics shall be made available to the Commission, to the ***European Parliament, to Member States, to the*** European Union Agency for Asylum ▌, to the European Border and Coast Guard Agency and to ***Europol***. The Commission shall, by means of implementing acts, specify the content of the monthly cross-system statistics. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 56(2).

Cross-system statistics alone shall not be used to deny access to the territory of the Union.

4. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects related to the application of this Regulation as well as the statistics pursuant to paragraph 1 and shall, upon request, make them available to a Member State ▌***,*** to the ***European Parliament, to the*** European Union Agency for Asylum***, to the European Border and Coast Guard Agency and to Europol***.

5. eu-LISA shall store the data referred to in paragraphs 1 to 4 of this Article, which shall not allow for the identification of individuals, for research and analysis purposes, thus enabling the authorities referred to in paragraph 3 of this Article to obtain customisable reports and statistics in the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/818.

6. Access to the central repository for reporting and statistics referred to in Article 39 of Regulation (EU) 2019/818 shall be granted to eu-LISA, to the Commission ▌ and to the authorities designated by each Member State in accordance with Article 40(2)***,*** to ***the*** authorised users of ***the European Union Agency for Asylum, of the European Border and Coast Guard Agency and of Europol,*** if such access is relevant for the implementation of their tasks.

Chapter II

Applicants for international protection

Article 15

Collection and transmission of biometric data

1. Each Member State shall take***, in accordance with Article 2(2),*** the biometric data of every applicant for international protection of at least six years of age ▌***:***

   (***a***) upon the registration of the application for international protection referred to in Article ***28*** of Regulation (EU) …/… ▌***[***Asylum Procedure Regulation ▌***]*** and shall, as soon as possible and no later than 72 hours ***from that registration,*** transmit them together with the ***other*** data referred to in Article 17***(1***) of this Regulation to ***Eurodac*** in accordance with Article 5(2)***; or***

   (b) ***upon the making of the application*** for international protection***, where the application is made at external border crossing points or in transit zones by a person who does not fulfil the entry conditions as set out in Article 6 of Regulation (EU) 2016/399, and shall, as soon as possible and no later than 72 hours after*** the biometric data ***have been*** taken ▌ transmit them together with the data referred to in Article 17(***1***) of this Regulation to ***Eurodac*** in accordance with Article 5(2) ▌ .

Non-compliance with the 72-hour time-limit shall not relieve Member States of the obligation to take and transmit the biometric data to ***Eurodac***. Where the condition of the fingertips does not allow the taking of the fingerprints of a quality ensuring appropriate comparison under Article 38, the Member State of origin shall retake the fingerprints of the applicant and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.

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

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

3. Where requested by the Member State concerned, the biometric data***, alphanumeric data and, where available, a scanned colour copy of an identity or travel document*** may also be taken and transmitted on behalf of that Member State by ***specifically trained*** members of the European Border and Coast Guard Teams or experts of the asylum support teams when exercising powers and performing their tasks in accordance with Regulation (EU) 2019/1896 and Regulation (EU) ***2021/2303***.

4. Each ▌ data ***set*** collected and transmitted in accordance with ***this Article*** shall be linked with other sets of data corresponding to the same third country national or stateless person in a sequence as set out in Article 5(6).

Article 16

Information on the status of the data subject

1. As soon as the Member State responsible has been determined in accordance with Regulation (EU) …/… [Regulation on Asylum and Migration Management] the Member State that conducts the procedures for determining the Member State responsible shall update its data set recorded pursuant to Article 17 of this Regulation regarding the person concerned by adding the Member State responsible.

   Where a Member State becomes responsible because there are reasonable grounds to consider the applicant a ***threat*** to ***the internal*** security ▌ of that Member State in accordance with Article 8(4) of Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] it shall update its data set recorded pursuant to Article 17 of this Regulation regarding the person concerned by adding the Member State responsible.

2. The following information shall be sent to ***Eurodac*** in order to be stored in accordance with Article 29***(1***) for the purpose of transmission under Articles 27 and 28:

(a) when an applicant for international protection or another person as referred to in Article 26(1), points (b) ▌ or (d) of Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] arrives in the Member State responsible following a transfer pursuant to a take back notification as referred to in Article 31 of that Regulation, the Member State responsible shall update its data set recorded in conformity with Article 17 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 30 of Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***], the Member State responsible shall send a data set recorded in conformity with Article 17 of this Regulation relating to the person concerned and shall include his or her date of arrival;

(c) ***as soon as the Member State of origin establishes that the person concerned whose data was recorded in Eurodac in accordance with Article 17 of this Regulation has left the territory of the Member States, it shall update its data set recorded in conformity with Article 17 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 Article 27(1a) of Regulation (EU) …/… [Regulation on Asylum and Migration Management];***

(***d***) as soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with Article 17 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 27(2) of Regulation (EU) …/… [Regulation on Asylum and Migration Management]***, it shall update its data set recorded in conformity with Article 17 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;

▌

3. Where responsibility shifts to another Member State, pursuant to Articles 27(1) and Article 58(3) of Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***], the Member State that establishes that responsibility has shifted, or the Member State of relocation, shall indicate the Member State responsible.

4. Where paragraphs 1 or 3 of this Article or Article 31(6) apply, ***Eurodac*** shall, as soon as possible and no later than within 72 hours, inform all Member States of origin of the transmission of such data by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 15(1), 18***(2)***, 20, 22(1), 23(1) or 24(1). Those Member States of origin shall also update the Member State responsible in their corresponding data sets.

Article 17

Recording of data

1. Only the following data shall be recorded in ***Eurodac in accordance with Article 5(2)***:

(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) date of birth;

(f) place of birth;

(g) Member State of origin, place and date of the application for international protection; in the cases referred to in Article 16(2)(b), the date of application shall be the one entered by the Member State who transferred the applicant;

(h) sex;

(i) where available, the type and number of identity or travel document, the three letter code of the issuing country and expiry date;

(j) where available, a scanned colour copy of an identity or travel document along with an indication of its authenticity or, where unavailable, another document which facilitates the identification of the third-country national or stateless person along with an indication of its authenticity;

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

▌

(l) date on which the biometric data were taken;

(m) date on which the data were transmitted to ***Eurodac;***

(n) operator user ID**.**

2. Additionally, where applicable and available, the following data shall be promptly recorded in Eurodac in accordance with Article 5(2):

(a) the Member State responsible in the cases referred to in Article 16(1), (2) or (3);

(b) the Member State of relocation in accordance with Article 25(1);

(c) ▌in the cases referred to in Article 16(2)(a), the date of the arrival of the person concerned after a successful transfer;

(d) ▌ in the cases referred to in Article 16(2)(b), the date of the arrival of the person concerned after a successful transfer;

(e) ▌ in the cases referred to in Article 16(2)(c), the date when the person concerned left ▌ the territory of the Member States;

(f) in the cases referred to in Article 16(2)(d), the date when the person concerned left or was removed from the territory of the Member States;

(g) in accordance with the cases referred to in Article 25(2), the date of arrival of the person concerned after a successful transfer;

(h) ***the fact*** that a visa was issued to the applicant, the Member State which issued or extended the visa or on behalf of which the visa has been issued and the visa application number;

(i) the fact that the person could pose a threat to internal security following the ***security check*** referred to in Regulation (EU) …/… [Screening Regulation] or following an examination pursuant ***to*** Article 8(4) of Regulation (EU) …/… [Regulation on Asylum and Migration Management] ***or to Article 10(5) of Regulation (EU) …/… [Asylum Procedure Regulation, if any of the following circumstances apply:***

(i) the person concerned is armed,

(ii) the person concerned is violent,

(iii) there are indications that the person concerned is involved in any of the offences referred to in Directive (EU) 2017/541,

(iv) there are indications that the person concerned is involved in any of the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA;

(j) ▌ the fact that the application for international protection has been rejected where the applicant has no right to remain and has not been allowed to remain in a Member State pursuant to Regulation (EU) …/… [Asylum Procedure Regulation];

(k***) the fact that, following an examination in the border procedure pursuant to Regulation (EU) …/… [Asylum Procedure Regulation], a decision rejecting an application for international protection as inadmissible, unfounded or manifestly unfounded, a decision rejecting or an act declaring an application as implicitly withdrawn or an act or a decision declaring an application as explicitly withdrawn has become final;***

(l) ▌ the fact that assistance for voluntary return and reintegration (AVRR) has been granted.

3. ***Where all the*** data ***in points (a)*** to ***(f) and (h) of*** paragraph 1 ***of this Article relating to a person as referred to in Article 15 are recorded in Eurodac, they shall be*** considered ***a data set transmitted to Eurodac*** for the ***purposes*** of Article 27(1)***, point (aa),*** of Regulation (EU) 818/2019 ▌.

4. ***The Member State of origin which concluded that the threat to internal security identified following the screening referred to in Regulation (EU) …/… [Screening Regulation] or following an examination pursuant to Article 8(4) of Regulation (EU) …/… (Regulation on Asylum and Migration Management) or to Article 10(5) of Regulation (EU) …/… [Asylum Procedure Regulation] no longer applies shall delete the record of the security flag from the dataset, after having consulted any other Member States having registered a dataset of the same person. Eurodac shall, as soon as possible and no later than 72 hours after the deletion of the security flag by another Member State of origin having produced a hit with data which they transmitted relating to persons as referred to in Articles 15(1), 22(1), 23(1) or 24(1), inform all Member States of origin of that deletion. Those Member State of origin shall also delete the security flag in the corresponding dataset.***

Chapter III

Persons registered for the purpose of conducting ***an admission procedure and persons admitted in accordance with a national resettlement scheme***

Section 1

Persons registered for the purpose of conducting an admission procedure ***under the Union Resettlement and Humanitarian Admission Framework***

Article 18

Collection and transmission of biometric data

1. Each Member State shall take and transmit to ***Eurodac*** the biometric data of every ▌ person of at least six years of age ***registered for the purpose of conducting an admission procedure under the Union Resettlement and Humanitarian Admission Framework*** as soon as possible from the registration referred to in Article ***9(3)*** of Regulation (EU) …/… [Resettlement Regulation] and at the latest before reaching the conclusion on admission referred to in Article ***9(9***) of Regulation (EU) …/… [Resettlement Regulation]. That obligation shall not apply if a Member State ▌ can reach that conclusion without a comparison of biometric data, where such a conclusion is negative.

2. Each Member State shall take the biometric data of every person of at least six years of age registered for the purpose of conducting an admission procedure under the Union Resettlement and Humanitarian Admission Framework and:

(a) whom that Member State grants international protection or a national humanitarian status in accordance with Regulation (EU) …/… [Resettlement Regulation];

(b) whom that Member State refuses to admit on one of the grounds referred to in Article 6(1)(f) of Regulation (EU) …/… [Resettlement Regulation];

(c) for whom that Member State discontinues the admission procedure due to the fact that that person does not give or withdraws his or her consent in accordance with Article 7 of Regulation (EU) …/… [Resettlement Regulation].

They shall transmit those biometric data together with the data referred to in Article 19(c) to (q) of this Regulation to Eurodac as soon as possible and no later than 72 hours after the decision to grant international protection or a national humanitarian status, to refuse admission or to discontinue the admission procedure.

3. Non-compliance with the ***deadlines*** set out in the first ***and second paragraphs*** shall not relieve Member States of the obligation to take biometric data and transmit them to ***Eurodac***. Where the condition of the fingertips does not allow the taking of the fingerprints of a quality ensuring appropriate comparison under Article 38, the Member State of origin shall retake the fingerprints ▌ and resend them as soon as possible after they have been successfully retaken.

Where it is not possible to take ▌ biometric data ▌ on account of measures taken to ensure his or her health or the protection of public health, Member States shall take and send such biometric data as soon as possible after those health grounds no longer prevail.

4. Where requested by the Member State concerned, the biometric data may, for the purpose of Regulation (EU) …/… [Resettlement Regulation], be taken and transmitted to the requesting Member State by another Member State, the European Union Agency for Asylum, or a relevant international organisation.

▌

5. ***For the purpose of this Article, the European Union Agency for Asylum (EUAA) and international organisations referred to in paragraph 4 shall not have access to Eurodac***.

▌

Article 19

Recording of data

Only the following data shall be recorded in ***Eurodac in accordance with Article 5(2)***:

(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) date of birth;

(f) place of birth;

(g) Member State of origin, place and date of the registration in accordance with Article ***9(3)*** of Regulation (EU) …/… [Resettlement Regulation];

(h) sex;

(i) where available, type and number of identity or travel document; three letter code of the issuing country and expiry date;

(j) where available, a scanned colour copy of an identity or travel document along with an indication of its authenticity, and if not available, another document which facilitates the identification of the third-country national or stateless person along with an indication of its authenticity;

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

(l) date on which the biometric data were taken;

(m) date on which the data were transmitted to ***Eurodac***;

(n) operator user ID;

(o) ***where applicable,*** the date of the ***decision to grant international protection or a national humanitarian status in accordance with Article 10(7)(a) or (aa) of*** Regulation (EU) …/… [Resettlement Regulation];

(p) ***where applicable,*** the date of the ***refusal of admission in accordance with*** Regulation (EU) …/… [Resettlement Regulation] and the ground ***on which admission was refused;***

(q) ***where applicable,*** the date ***of the discontinuation of*** the admission procedure ▌ as referred to in Regulation (EU) …/… [Resettlement Regulation].

Where all the data ***in points (a) to (f) and (h), of*** paragraph 1 ***of this Article relating to a person as referred to in Article 18(2) are recorded in Eurodac, they shall be*** considered ***a data set transmitted to Eurodac*** for the ***purposes*** of Article 27(1)***, point (aa),*** of Regulation (EU) 818/2019 ▌.

Section 2

Persons admitted in accordance with a national resettlement scheme

Article 20

Collection and transmission of biometric data

Each Member State shall take the biometric data of every ▌ person of at least six years of age ***who has been admitted in accordance with a national resettlement scheme*** and transmit such data to ***Eurodac***, together with the data referred to in Article 21(c) to (o) of this Regulation as soon as ***they grant that person*** international protection or a ***national*** humanitarian status ▌ and no later than 72 hours thereafter.

Non-compliance with the deadline set out in the first subparagraph shall not relieve Member States of the obligation to take and transmit the biometric data to ***Eurodac***. Where the condition of the fingertips does not allow the taking of the fingerprints of a quality ensuring appropriate comparison under Article 38, the Member State of origin shall retake the fingerprints ▌ and resend them as soon as possible after they have been successfully retaken.

By way of derogation from the second subparagraph, where it is not possible to take biometric data of a person admitted in accordance with a national resettlement scheme on account of measures taken to ensure his or her health or the protection of public health, Member States shall take and send such ***biometric data*** as soon as possible and no later than 48 hours after those health grounds no longer prevail.

▌

Article 21

Recording of data

Only the following data shall be recorded in ***Eurodac in accordance with Article 5(2)***:

(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) date of birth;

(f) place of birth;

(g) Member State of origin, place and date of the registration;

(h) sex;

(i) where available, type and number of identity or travel document ▌**,** three letter code of the issuing country and expiry date;

(j) where available, a scanned colour copy of an identity or travel document along with an indication of its authenticity, and if not available, another document which facilitates the identification of the third-country national or stateless person along with an indication of its authenticity;

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

(l) date on which the biometric data were taken;

(m) date on which the data were transmitted to ***Eurodac***;

(n) operator user ID;

(o) date on which international protection or a humanitarian status under national law was granted.

Where all the data ***in points (a) to (f), and (h) of*** paragraph 1 ***of this Article relating to a person referred to in Article 20 are recorded in Eurodac, they shall be*** considered ***a data set transmitted to Eurodac*** for the ***purposes*** of Article 27(1) ***point (aa)*** of Regulation (EU) 818/2019 ▌ .

Chapter IV

Third-country nationals or stateless persons apprehended in connection with the irregular crossing of an external border

Article 22

Collection and transmission of biometric data

1. Each Member State shall promptly take***, in accordance with Article 2(2),*** the biometric data of every third-country national or stateless person of at least six years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn him or her back.

2. The Member State concerned shall, as soon as possible and no later than 72 hours after the date of apprehension, transmit to ***Eurodac in accordance with Article 5(2)*** the following data in relation to any third-country national or stateless person, as referred to in paragraph 1, who is not turned back:

   (a) fingerprint data;

(b) a facial image;

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

(d) nationality(ies);

(e) date of birth;

(f) place of birth;

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

(h) sex;

(i) where available, type and number of identity or travel document; three letter code of the issuing country and expiry date;

(j) where available, a scanned colour copy of an identity or travel document along with an indication of its authenticity or, where unavailable, another document which facilitates the identification of the third-country national or stateless person along with an indication of its authenticity;

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

(l) date on which the biometric data were taken;

(m) date on which the data were transmitted to ***Eurodac***;

(n) operator user ID;

3. ***Additionally,*** where applicable ***and available, the following data shall be promptly transmitted to Eurodac in accordance with Article 5(2):***

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

(b) the Member State of relocation in accordance with Article 25(1);

(c) ▌ the fact that assistance for voluntary return and reintegration (AVRR) has been granted,

(d) the fact that the person could pose a threat to internal security***,*** following the screening referred to in Regulation (EU) …/… [Screening Regulation]***, if any of the following circumstances apply:***

(i) the person concerned is armed,

(ii) the person concerned is violent,

(iii) there are indications that the person concerned is involved in any of the offences referred to in Directive (EU) 2017/541,

(iv) there are indications that the person concerned is involved in any of the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA.

4. 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.

5. Non-compliance with the 72 hour time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data to ***Eurodac***. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 38, 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.

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

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

7. 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.

8. Where requested by the Member State concerned, the biometric data***, alphanumeric data and, where available, a scanned colour copy of an identity or travel document*** may also be taken and transmitted on behalf of that Member State by ***specifically trained*** members of the European Border and Coast Guard Teams or experts of the asylum support teams when exercising powers and performing their tasks in accordance with Regulation (EU) 2019/1896 and Regulation (EU) ***2021/2303***.

9. Each data set collected and transmitted in accordance with paragraph 1 ***this Article*** shall be linked with other sets of data corresponding to the same third country national or stateless person in a sequence as set out in Article 5(6).

10. ***Where all the*** data ***in points (a)*** to ***(f) and (h) of*** paragraph 2 ***of this Article relating to a person as referred to in paragraph 1 of this Article are recorded in Eurodac, they shall be*** considered ***a data set transmitted to Eurodac*** for the ***purposes*** of Article 27(1)***, point (aa),*** of Regulation (EU) 818/2019 ▌.

Chapter V

Third-country nationals or stateless persons illegally staying in a member state

Article 23

Collection and transmission of biometric data

1. Each Member State shall promptly take***, in accordance with Article 2(2),*** the biometric data of every third-country national or stateless person of at least six years of age who is illegally staying within its territory.

2. The Member State concerned shall, as soon as possible and no later than 72-hours after the third-country national or the stateless person has been found to be illegally staying, transmit to ***Eurodac in accordance with Article 5(2)*** 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) date of birth;

(f) place of birth;

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

(h) sex;

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

(j) where available, a scanned colour copy of an identity or travel document along with an indication of its authenticity or, where unavailable, another document which facilitates the identification of the third-country national or stateless person along with an indication of its authenticity;

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

(l) date on which the biometric data were taken;

(m) date on which the data were transmitted to ***Eurodac***;

(n) operator user ID;

3. ***Additionally,*** where applicable ***and available, the following data shall be promptly transmitted to Eurodac, as appropriate*** in accordance with ***Article 5(2):***

(a) ***in accordance with*** paragraph 6, the date when the person concerned left or was removed from the territory of the Member States;

(b) the Member State of relocation in accordance with Article 25(1);

(c) where applicable, in accordance with the cases referred to in Article 25(2), the date of arrival of the person concerned after a successful transfer;

(d) ▌ the fact that assistance for voluntary return and reintegration (AVRR) has been granted;

(e) ▌ the fact that the person could pose a threat to internal security***,*** following the screening referred to in Regulation (EU) …/… [Screening Regulation]***, or following a security check carried out at the moment of taking of the biometric data foreseen in Article 23(1) if any of the following circumstances apply:***

(i) ***the person concerned is armed,***

(ii) ***the person concerned is violent,***

(iii) there are indications that the person concerned is involved in any of the offences referred to in Directive (EU) 2017/541,

(iv) there are indications that the person concerned is involved in any of the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA.

4. Non-compliance with the 72 hour time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data to ***Eurodac***. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 38, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.

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

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

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

7. Each data set collected and transmitted in accordance with ***this Article*** shall be linked with other sets of data corresponding to the same third country national or stateless person in a sequence as set out in Article 5(6).

8. ***Where all the*** data ***in points (a)*** to ***(f) and (h) of*** paragraph 2 ***of this Article relating to a person as referred to in paragraph 1 of this Article are recorded in Eurodac, they shall be*** considered ***a data set transmitted to Eurodac*** for the ***purposes*** of Article 27(1)***, point (aa),*** of Regulation (EU) 818/2019 ▌ .

Chapter VI

Third-country nationals or stateless persons disembarked following a search and rescue operation

Article 24

Collection and transmission of biometric data

1. Each Member State shall promptly take the biometric data of every third-country national or stateless person of at least six years of age who is disembarked following a search and rescue operation as defined in Regulation (EU) …/… [Regulation on Asylum and Migration Management].

2. The Member State concerned shall, as soon as possible and no later than 72 hours after the date of disembarkation, transmit to ***Eurodac in accordance with Article 5(2)***, 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) date of birth;

(f) place of birth;

(g) Member State of origin, place and date of disembarkation;

(h) sex;

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

(j) date on which the biometric data were taken;

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

(l) operator user ID;

3. ***Additionally,*** where ***applicable and*** available, ***the following data shall be transmitted to Eurodac in accordance with Article 5(2) as soon as available:***

(a) type and number of identity or travel document; three letter code of the issuing country and expiry date;

(***b***) ▌ a scanned colour copy of an identity or travel document along with an indication of its authenticity or, where unavailable, another document which facilitates the identification of the third-country national or stateless person along with an indication of its authenticity;

▌

(c) in accordance with paragraph 8, the date when the person concerned left or was removed from the territory of the Member States;

(d) the Member State of relocation in accordance with Article 25(1);

(e) ▌ the fact that assistance for voluntary return and reintegration (AVRR) has been granted,

(f) the fact that the person could pose a threat to internal security following the screening referred to in Regulation (EU) …/… [Screening Regulation]***, if any of the following circumstances apply:***

(i) the person concerned is armed,

(ii) the person concerned is violent,

(iii) there are indications that the person concerned is involved in any of the offences referred to in Directive (EU) 2017/541,

(iv) there are indications that the person concerned is involved in any of the offences referred to in Article 2(2) of Framework Decision 2002/584/JHA.

4. Non-compliance with the ▌ time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data to ***Eurodac***. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 38, the Member State of origin shall retake the fingerprints of persons disembarked as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.

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

6. 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.

7. ***In case of sudden influx, Member States may extend the 72-hour time-limit in paragraph 2 by a maximum of a further 48 hours. This derogation enters into force the day it is notified to the Commission and to the other Member States and for the duration foreseen in the notification. The duration stated in the notification shall not exceed one month.***

8. 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.

9. Where requested by the Member State concerned, the biometric data***, alphanumeric data and, where available, a scanned colour copy of an identity or travel document*** may also be taken and transmitted on behalf of that Member State by ***specifically trained*** members of the European Border and Coast Guard Teams or experts of the asylum support teams when exercising powers and performing their tasks in accordance with Regulation(EU) 2019/1896 and Regulation (EU) ***2021/2303.***

10. Each data set collected and transmitted in accordance with this Article shall be linked with other sets of data corresponding to the same third country national or stateless person in a sequence as set out in Article 5(6).

11. Without prejudice to the application of Regulation (EU) …/… [***Regulation on Asylum and Migration Management], the fact that the data of a person is transmitted to Eurodac in accordance with this Article shall not result in any discrimination difference of treatment of a person covered by Article 22(1) of this Regulation***.

12. ***Where all the data in points (a) to (f) and (h) of paragraph 2 of this Article relating to a person as referred*** to ***in*** paragraph 1 ***of this Article are recorded in Eurodac, they shall be*** considered ***a data set transmitted to Eurodac*** for the ***purposes*** of Article 27(1)***, point (aa),*** of Regulation (EU) 818/2019 ▌.

Chapter VII
Information on Relocation

Article 25
Information on the status of relocation of the data subject

1. As soon as the Member State of relocation is obliged to relocate the person concerned pursuant to Article 57(7) of Regulation (EU) …/… [Regulation on Asylum and Migration Management], the benefiting Member State shall update its data set recorded pursuant to Articles 17, 22, 23 or 24 of this Regulation relating to the person concerned by adding the Member State of relocation.

2. When a person arrives in the Member State of relocation following the confirmation by the Member State of relocation to relocate the person concerned pursuant to Article 57(7) of Regulation (EU) …/… [Regulation on Asylum and Migration Management], that Member State shall send a data set recorded in conformity with Articles 17 or 23 of this Regulation relating to the person concerned and shall include his or her date of arrival. The data set shall be stored in accordance with Article 29(1) for the purpose of transmission under Articles 27 and 28.

Chapter VIII

Beneficiaries of temporary protection

Article 26

Collection and transmission of biometric data

1. Each Member State shall promptly take the biometric data of every third-country national or stateless person of at least six years of age registered as beneficiary of temporary protection in the territory of that Member State pursuant to Directive 2001/55/EC.

2. The Member State concerned shall, as soon as possible and no later than 10 days after the registration as beneficiary of temporary protection, transmit to Eurodac in accordance with Article 5(2), 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) date of birth;

(f) place of birth;

(g) Member State of origin, place and date of registration as beneficiary of temporary protection ;

(h) sex;

(i) where available, the type and number of identity or travel document, the three letter code of the issuing country and expiry date;

(j) where available, a scanned colour copy of an identity or travel document along with an indication of its authenticity or, where unavailable, another document;

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

(l) date on which the biometric data were taken;

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

(n) operator user ID;

(o) where relevant, the fact that the person previously registered as beneficiary of temporary protection falls under one of the exclusion grounds pursuant to Article 28 of Directive 2001/55/CE;

(p) reference of the relevant Council Implementing Decision;

3. Non-compliance with the 10 day time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data to Eurodac. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 38, the Member State of origin shall retake the fingerprints of the beneficiary of temporary protection 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.

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

In the event of serious technical problems, Member States may extend the 10 day time-limit in paragraph 2 by a maximum of a further 48 hours in order to carry out their national continuity plans.

5. Where requested by the Member State concerned, the biometric data may also be taken and transmitted on behalf of that Member State by members of the European Border and Coast Guard Teams or experts of the asylum support teams when exercising powers and performing their tasks in accordance with Regulation (EU) 2019/1896 and Regulation (EU) 2021/2303 EU Agency for Asylum Regulation.

6. Each data set collected and transmitted in accordance with paragraph 1 this Article shall be linked with other sets of data corresponding to the same third country national or stateless person in a sequence as set out in Article 5(6).

7. Where all the data in points (a) to (f) and (h), of paragraph 2 of this Article relating to a person as referred to in paragraph 1 of this Article are recorded in Eurodac, they shall be considered a data set transmitted to Eurodac for the purposes of Article 27(1), point (aa), of Regulation (EU) 818/2019.

Chapter IX

Procedure for comparison of data for applicants for international protection, third-country nationals and stateless persons apprehended crossing the border irregularly or illegally staying in the territory of a member state, third-country nationals and stateless persons registered for the purpose of conducting an admission procedure and admitted in accordance with a national resettlement scheme**,** third-country nationals and stateless persons disembarked following a search and rescue operation ***and beneficiaries of temporary protection***

Article 27

Comparison of biometric data

1. Biometric data transmitted by any Member State, with the exception of those transmitted in accordance with ***Articles 16(2***)(b) ***and (c), 18 and 20***, shall be compared automatically with the biometric data transmitted by other Member States and already stored in ***Eurodac*** in accordance with Articles 15(1), 18***(2)***, 20, 22(1), ***and 23***(1)**▌,** 24a(1) ***and 26(1).***

2. ***Biometric data transmitted by any Member State in accordance with Article 18(1) shall be compared automatically with the biometric data transmitted by other Member States and already stored in Eurodac in accordance with Articles 15(1) that are marked in accordance with Article 31, and with Articles 18(2) and 20***.

3. ***Eurodac*** shall ensure, at the request of a Member State, that the comparison referred to in paragraph 1 of this Article covers the biometric data previously transmitted by that Member State, in addition to the biometric data from other Member States.

4. ***Eurodac*** 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 38(4). Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in ***Article 17***, 18 ▌, 21 ▌, 22(2), 23(2)***, 24(2)*** and 26(2) along with, where appropriate, the mark referred to in Article 31(1) and (4). Where a negative result is received, the data referred to in ***Article 17***, 19 ▌, 21 ▌, 22(2), 23(2)***, 24(2)*** and 26(2) shall not be transmitted.

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

Article 28

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 38 or where no fingerprints are available for comparison, a Member State shall carry out a comparison of facial image data.

2. Facial image data and data relating to the sex of the data-subject may be compared automatically with the facial image ▌ and ***the*** personal data relating to the sex of the data-subject transmitted by other Member States and already stored in ***Eurodac*** in accordance with ***Article*** 15(1), 18***(2)***, 20, 22(1), ***and 23***(1), 24***(1)*** and 26(1) with the exception of those transmitted in accordance with ***Articles 16(2)***(b) ***and (c), 18(2) and 20***.

Eurodac shall ensure, at the request of a Member State that the comparison referred to in paragraph 1 of this Article covers the facial image ▌ previously transmitted by that Member State, in addition to the facial image data from other Member States.

3. Facial image data and data relating to the sex of the data-subject transmitted by any Member State in accordance with Article 18(1) may be compared automatically with the facial image and the personal data relating to the sex of the the data-subject transmitted by other Member States and already stored in Eurodac in accordance with Articles 15(1), that are marked in accordance with Article 31, and with Articles 18(2) and 20.

4. ***Eurodac*** 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 38(5). Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Articles 17, 19 ▌, 21 ▌, 22(2), 23(2)***, 24*** and 26(2) along with, where appropriate, the mark referred to in Article 31(1) and (4). Where a negative hit result is received, the data referred to in Articles 17, 19 ▌, 21 ▌, 22(2), 23(2)***, 24(2)*** and 26(2) shall not be transmitted.

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

Chapter X

Data storage, advanced data erasure and marking of data

Article 29

Data storage

1. For the purposes laid down in Article 15(1), each set of data relating to an applicant for international protection, as ***referred to in Article 17, shall be stored in Eurodac*** for ten years from the date on which the biometric data were ***transmitted***.

2. The biometric data referred to in Article 18(1) shall not be recorded in Eurodac.

3. For the purposes laid down in Article 18(***2***), each set of data ***as referred to in Article 19*** relating to a third-country national or stateless person ***as*** referred to in Article 18***(2)(a)***, shall be stored in ***Eurodac*** for ***five*** years from the date on which the biometric data were ***transmitted***.

4. For the purposes laid down in Article 18(2), each set of data as referred to in Article 19 relating to a third-country national or stateless person as referred to in Article 18(2)(b) or (c), shall be stored in Eurodac for three years from the date on which the biometric data were transmitted.

5. For the purposes laid down in Article 20, each set of data relating to a third-country national or stateless person ***to be*** admitted in accordance with a national resettlement scheme, ***as*** referred to in Article 21, shall be stored in ***Eurodac*** for ***five*** years from the date on which the biometric data were ***transmitted***.

6. For the purposes laid down in Article 22(1), each set of data relating to a third-country national or stateless person as referred to in Article 22(2) shall be stored in ***Eurodac*** for five years from the date on which his or her biometric data were ***transmitted***.

7. For the purposes laid down in Article 23(1), each set of data relating to a third-country national or stateless person as referred to in Article 23(2) shall be stored in ***Eurodac*** for five years from the date on which his or her biometric data were ***transmitted***.

8. For the purposes laid down in Article 24(1), each set of data relating to a third-country national or stateless person as referred to in Article 24(2) shall be stored in ***Eurodac*** as appropriate for five years from the date on which his or her biometric data were ***transmitted***.

9. ***For the purposes laid down in Article 26(1), each set of*** data relating to a ***third country national or stateless*** person ▌ as referred to in Article 26(***2***) shall be stored in ***Eurodac*** for ***one year*** from the date of ***the entry into force of the relevant Council Implementing Decision. The retention period shall be extended yearly for the duration of the temporary protection***.

10. Upon expiry of the data storage periods referred to in paragraphs 1 to 9 of this Article, the data of the data-subjects shall be ***automatically erased*** from ***Eurodac***.

Article 30

Advanced data erasure

1. Data relating to a person who has acquired the citizenship of a Member State of origin before the expiry of the period referred to in Article 29(1), (3), (5), (6), (7), ▌ (8) or (9) shall be erased from the ***Eurodac*** without delay by that Member State in accordance with Article 28(3).

   Data relating to a person who has acquired the citizenship of ***another*** Member State ▌ before the expiry of the period referred to in Article 29(1), (3), (5), (6), (7), (8) ▌ or (9) shall be erased from the ***Eurodac*** by the Member State of origin, in accordance with Article 40(3), as soon as it becomes aware of the fact that the person concerned has acquired such citizenship.

2. ***Eurodac*** 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 Articles 15(1), 18, 20, 22(1), 23(1)***, 24(1)*** or 26***(1***).

▌

Article 31

Marking▌ of data

1. For the purposes laid down in Article ***1(1***)(a)▌, the Member State of origin which granted international protection▌ to a person whose data were previously recorded in ***Eurodac*** pursuant to Article 17▌ shall mark the relevant data in conformity with the requirements for electronic communication with ***Eurodac*** established by eu-LISA. That mark shall be stored in ***Eurodac*** in accordance with Article 29(1)▌ for the purpose of transmission under Article 27 ***and 28***▌. ***Eurodac*** 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 15(1), 18***(2), 20***, 22(1), 23(1)***, 24(1)*** or 26***(1***). Those Member States of origin shall also mark the corresponding data sets.

2. The data of beneficiaries of international protection stored in ***Eurodac in accordance with Article 5(2)*** and marked pursuant to paragraph 1 of this Article shall be made available for comparison for the purposes laid down in Article 1(1)(e) until such data is automatically erased from ***Eurodac*** in accordance with Article 29(10).

3. The Member State of origin shall unmark data concerning a third-country national or stateless person whose data were previously marked in accordance with paragraphs 1 or 2 of this Article if his or her status is withdrawn under Articles 14 or ***19*** of Regulation (EU) …/… [Qualification Regulation].

4. For the purposes laid down in Article 1(1)(a) and (c), the Member State of origin which issued a residence document to an illegally staying third-country national or stateless person whose data were previously recorded in ***Eurodac*** as appropriate pursuant to Article 22***(2***) and 23(2)***,*** or to a third-country national or stateless person disembarked following a search and rescue operation whose data were previously recorded in the ***Eurodac as appropriate*** pursuant to Article 24(2)***, or to a beneficiary of temporary protection whose data were previously recorded in Eurodac as appropriate pursuant to Article 26(2***) shall mark the relevant data in accordance with the requirements for electronic communication with ***Eurodac*** established by eu-LISA. That mark shall be stored in ***Eurodac*** in accordance with Article 29(6), (7)***, (8)*** and (9) for the purpose of transmission under Article 27 and 28. ***Eurodac*** 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 15(1), 22(1), 23(1)***, 24(1)*** or 26(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 ***Eurodac*** and marked pursuant to paragraph 4 of this Article shall be made available for comparison for the purposes laid down in Article 1(1)(e) until such data is automatically erased from ***Eurodac*** in accordance with Article 29(10).

6. For the purposes of Article 58(4) of Regulation (EU) …/… [Regulation on Asylum and Migration Management], the Member State of relocation shall, following the registration of the data pursuant to Article 25(2), register itself as the Member State responsible and mark that data with the marking introduced by the Member State who granted protection.

Chapter XI

Procedure for comparison and data transmission for law enforcement purposes

Article 32

Procedure for comparison of biometric or alphanumeric data with Eurodac data

1. For the purposes laid down in Article 1(1)(e), the designated authorities referred to in Articles 7***(1***) and 9***(1***) may submit a reasoned electronic request as provided for in Article 33(1) and in Article 34(1) together with the reference number used by them, to the verifying authority for the transmission for comparison of biometric data or alphanumeric data to ***Eurodac*** via the National Access Point or Europol 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 33 or 34, as appropriate, are fulfilled.

2. Where all the conditions for requesting a comparison referred to in Articles 33 or 34 are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point or Europol Access Point which will process it to ***Eurodac*** in accordance with Articles 27 and 28 for the purpose of comparison with the biometric or alphanumeric data transmitted to the ***Eurodac*** pursuant to Articles 15(1), 18, 20, 22(1), 23(1)***, 24(1)*** and 26(1).

3. A comparison of a facial image with other facial image data in ***Eurodac*** pursuant to Article 1(1)(e) may be carried out in accordance with Article 28(1), if such data is available at the time the reasoned electronic request is made pursuant to Article 33(1) or Article 34***(1***).

4. In exceptional cases of urgency where there is a need to prevent an imminent danger associated with a terrorist offence or other serious criminal offence, the verifying authority may transmit the biometric or alphanumeric data to the National Access Point or Europol 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 33 or Article 34 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.

5. Where an ex-post verification determines that the access to Eurodac data was not justified, all the authorities that have accessed such data shall erase the information communicated from Eurodac and shall inform the verifying authority of such erasure.

Article 33

Conditions for access to Eurodac by designated authorities

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

– national databases; and

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

and where the following cumulative conditions are met:

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

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

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

In addition to the prior check of the databases referred to in the first subparagraph, designated authorities may also conduct a check in the Visa Information System, provided that the conditions for a comparison with the data stored therein, as laid down in Decision 2008/633/JHA, are met. Designated authorities may submit the reasoned electronic request referred to in the first subparagraph at the same time they submit a request for comparison with the data stored in the Visa Information System.

2. Where the designated authorities consulted the CIR in accordance with Article 22(1) of Regulation (EU) 2019/818, ***and, in accordance with paragraph 2 of that*** Article***,*** the ***CIR indicated*** that data ***on the person concerned*** is stored in Eurodac***, the designated authorities may have access to Eurodac for consultation without a prior check in national databases and in the automated fingerprinting identification systems of all other Member States***.

3. Requests for comparison with Eurodac data for the purposes of Article 1(1)(e) shall be carried out with biometric or alphanumeric data.

Article 34

Conditions for access to Eurodac by Europol

1. For the purposes laid down in Article 1(1)(e), Europol's designated authority may submit a reasoned electronic request for the comparison of biometric or alphanumeric data with the data stored in ***Eurodac*** within the limits of Europol's mandate and where necessary for the performance of Europol's tasks only if comparisons with biometric or alphanumeric 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 including specific persons; and

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

2. Where Europol consulted the CIR in accordance with Article 22(1) of Regulation ***(EU)*** 2019/818, they may access Eurodac for consultation under the conditions foreseen in this Article where the reply received pursuant to Article 22(2) of Regulation (EU) ***2019/818 indicates*** that data is stored in Eurodac.

3. Requests for comparison with Eurodac data for the purposes of Article 1(1)(e) shall be carried out with biometric or alphanumeric data.

4. 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 35

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

1. Without prejudice to Article 39, all communication between the designated authorities, the verifying authorities, the National Access Points and the Europol Access Point shall be secure and take place electronically.

2. For the purposes laid down in Article 1(1)(e), searches with biometric or alphanumeric data shall be digitally processed by the Member States and Europol and transmitted in the data format as set out in the agreed Interface Control Document, in order to ensure that the comparison can be carried out with other data stored in ***Eurodac***.

Chapter XII

Data processing, data protection and liability

Article 36

Responsibility for data processing

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

(a) biometric data and the other data referred to in Articles 17***, Article*** 19 ▌, ***Article*** 21 ▌, ***Article*** 22(2), ***Article*** 23(2), ***Article 24(2)*** and ***Article 26***(2) are taken lawfully;

(b) biometric data and the other data referred to in ***Article 17***, ***Article 19*** ▌, 21 ▌, ***Article*** 22(2), ***Article 23***(2) ▌***, Article*** 24(2) ***and Article 26(2)*** are lawfully transmitted to ***Eurodac***;

(c) data are accurate and up-to-date when they are transmitted to ***Eurodac***;

(d) without prejudice to the responsibilities of eu-LISA, data in ***Eurodac*** are lawfully recorded, stored, rectified and erased;

(e) the results of biometric data comparisons transmitted by ***Eurodac*** are lawfully processed.

2. In accordance with Article 48, the Member State of origin shall ensure the security of the data referred to in paragraph 1 before and during transmission to ***Eurodac*** as well as the security of the data it receives from ***Eurodac***.

3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article 38(4).

4. eu-LISA shall ensure that ***Eurodac*** is operated, including where operated for testing purposes, in accordance with the provisions of this Regulation and of relevant Union data protection rules. In particular, eu-LISA shall:

   (a) adopt measures ensuring that all persons, including contractors, working with ***Eurodac*** 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 ***Eurodac*** in accordance with Article 48;

   (c) ensure that only persons authorised to work with ***Eurodac*** have access thereto, without prejudice to the competences of the European Data Protection Supervisor.

   eu-LISA shall inform the European Parliament and the Council as well as the European Data Protection Supervisor of the measures it takes pursuant to the first subparagraph.

Article 37

Transmission

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

2. Member States shall transmit the data referred to in ***Article 17, Article*** 19 ▌, ***Article*** 21 ▌, ***Article*** 22(2), ***Article 23***(2), ***Article 24(2)*** and ***Article 26***(2) electronically. The data referred to in ***Article 17, Article*** 19 ▌, ***Article*** 21 ▌, ***Article*** 22(2), ***Article 23***(2), ***Article 24(2)*** and ***Article 26***(2) shall be automatically recorded in ***Eurodac***. As far as necessary for the efficient operation of ***Eurodac***, eu-LISA shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to ***Eurodac*** and vice versa***.***

3. The reference number referred to in Articles 17***(1)***(***k***), 19(k), 21(k), 22(2)(***k***), 23***(2)(k), 24(2)(i), 26(2***)(k) and 32***(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 Articles 15(1), 18, 20, 22(1), 23(1), ***Article 24*** or ***Article 26***.

4. The reference number shall begin with the identification letter or letters by which the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person or request. '1' refers to data relating to persons referred to in Article 15(1), '2' to persons referred to in Article 22(1), '3' to persons referred to in Article 23(1), '4' to requests referred to in Article 33, '5' to requests referred to in Article 34,'***6***' to requests referred to in Article 43, '***7***' to requests referred to in Article 18 ***and*** '***8***' to persons referred to in Article 20***,*** '***9***' to ***persons*** referred to in Article 24***(1) and '10' to persons referred to in Article 26***(1).

5. eu-LISA shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by ***Eurodac***.

6. ***Eurodac*** 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 38

Carrying out comparisons and transmitting results

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

2. ***Eurodac*** 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, ***Eurodac*** 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 ***Eurodac***, the ***Agency*** eu-LISA shall establish criteria to ensure the priority handling of requests.

3. As far as necessary for the efficient operation of ***Eurodac***, eu-LISA shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.

4. Where necessary, a fingerprint expert in the receiving Member State, as defined in accordance with its national rules and specifically trained in the types of fingerprint comparisons provided for in this Regulation, shall immediately check the result of the comparison of fingerprint data carried out pursuant to Article 27.

   Where, following a comparison of both fingerprint and facial image data with data recorded in the computerised central database, ***Eurodac*** returns a fingerprint hit and a facial image hit, Member States may check the result of the comparison of the facial image data.

For the purposes laid down in Article 1(1)(a), (b) and (c) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.

5. The result of the comparison of facial image data carried out pursuant to Article 27, where a hit based on a facial image is received only, and Article 16 shall be immediately checked and verified in the receiving Member State by an expert trained in accordance with national practice. For the purposes laid down in Article 1(1)(a), (b) and (c) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.

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

6. Where final identification in accordance with paragraphs 4 and 5 reveals that the result of the comparison received from ***Eurodac*** does not correspond to the biometric data sent for comparison, Member States shall immediately erase the result of the comparison and communicate this fact as soon as possible and no later than after three working days to eu-LISA and inform them of the reference number of the Member State of origin and the reference number of the Member State that received the result.

Article 39

Communication between Member States and ***Eurodac***

Data transmitted from the Member States to ***Eurodac*** and vice versa shall use the Communication Infrastructure. As far as is necessary for the efficient operation of ***Eurodac***, eu-LISA shall establish the technical procedures necessary for the use of the Communication Infrastructure.

Article 40

Access to, and rectification 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 ***Eurodac*** 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 27 and 28.

2. The authorities of Member States which, pursuant to paragraph 1 of this Article, have access to data recorded in ***Eurodac*** shall be those designated by each Member State for the purposes laid down in Article 1(1)(a), (b)***,*** and (c). That designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and eu-LISA a list of those units and any amendments thereto. eu-LISA shall publish the consolidated list in the *Official Journal of the European Union*. Where there are amendments thereto, eu-LISA shall publish once a year an updated consolidated list online.

3. Only the Member State of origin shall have the right to amend the data which it has transmitted to ***Eurodac*** by rectifying or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article 29.

4. Access for the purposes of consulting the Eurodac data stored in the CIR shall be granted to the duly authorised staff of the national authorities of each Member State and to the duly authorised staff of the Union bodies competent for the purposes laid down in ***Articles*** 20 and ▌21 of Regulation ***(EU)*** 2019/818. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and ***Union*** bodies in accordance with those purposes and shall be proportionate to the objectives pursued.

5. If a Member State or eu-LISA has evidence to suggest that data recorded in ***Eurodac*** are factually inaccurate, it shall, without prejudice to the notification of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, advise the Member State of origin as soon as possible.

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

6. eu-LISA shall not transfer or make available to the authorities of any third country data recorded in ***Eurodac***. This prohibition shall not apply to transfers of such data to third countries to which Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] applies.

Article 41

Keeping of records

1. eu-LISA shall keep records of all data processing operations within ***Eurodac***. 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. For the purposes of Article 10, eu-LISA shall keep records of each data processing operation carried out within Eurodac. Records of such ***type*** of operations shall include the elements provided for in the first paragraph and the hits triggered while carrying out the automated processing laid down in Article 20 of Regulation (EU) 2018/1240.

3. For the purpose of Article 12, Member States and eu-LISA shall keep records of each data processing operation carried out within Eurodac and the Visa Information System in accordance with this Article and ▌ Article 34 of Regulation (EC) No 767/2008.

4. 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 46. 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 29 has expired, unless they are required for monitoring procedures which have already begun.

5. For the purposes laid down in Article 1(1)(a), (b) ▌**,** (c), ***(g), (h) and (j),*** each Member State shall take the necessary measures in order to achieve the objectives set out in paragraphs 1***, 2, 3*** and 4 of this Article in relation to its national system. In addition ▌ each Member State shall keep ***record*** of the staff duly authorised to enter or retrieve the data.

Article 42

Rights of information

1. A person covered by Articles 15(1), 18, 20, ***Article 22***(1), ***Article 23***(1), ***Article 24(1)*** or ***Article 26***(1) shall be informed by the Member State of origin in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand in a concise, transparent, intelligible and easily accessible form, using clear and plain language, of the following:

(a) the identity and contact details of the controller within the meaning of Article 4(7) of Regulation (EU) 2016/679 and of his or her representative, if any and the contact details of the data protection officer;

(b) ▌ data will be processed in Eurodac and the legal basis of processing, including a description of the aims of Regulation (EU) …/… [▌ Asylum and Migration Management], in accordance with Article 6 thereof and where applicable, of the aims of Regulation (EU) …/… [Resettlement Regulation], and an explanation in intelligible form of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;

▌

(c) ***in relation to a person covered by Articles 15(1), 22(1), 23(1) or 24(1), the fact that if a security check as referred to in Articles 17(2)(i), 22(3)(d), 23(3)(e) shows that he or she could pose a threat to internal security, the Member State of origin shall register that in Eurodac;***

(d) ***the recipients or categories of recipients of the data of the data, if any;***

(e) ***in relation to a person covered by Articles 15(1), 18***, 20, ***22***(1)***,*** 23(1)***, 24(1) or 26(1)***, the obligation to have his or her biometric data taken and the relevant procedure, including the possible implications of non-compliance with such an obligation;

(f) the period for which the data will be stored pursuant to Article 29;

(g) the existence of the right to request from the controller access to data relating to him or her, and the right to request that inaccurate data relating to him or her be rectified and the completion of incomplete personal data or that unlawfully processed personal data concerning him or her be erased or restricted, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the supervisory authorities referred to in Article 44(1);

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

2. In relation to a person covered by Articles 15(1), 18, 20, 22(1), 14(1), 24***(1)*** and 26(1) ▌ the information referred to in paragraph 1 of this Article shall be provided at the time when his or her biometric data are taken.

Where a person covered by ***Article*** 15(1), ***Article 18***, ***Article*** 20, ***Article 22***(1)***,*** ***Article*** 23(1)***, Article 24(1) and Article 26(1)*** is a minor, the information shall be provided by Member States in an age-appropriate manner.

The procedure to capture biometric data shall be explained to minors by using leaflets, infographics or demonstrations, or a combination of any of the three, as appropriate, specifically designed in such a way as to ensure that minors ***understands*** it.

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) …/… [▌ Asylum and Migration Management ***Regulation***] 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 administrative measures for ensuring compliance with providing biometric data, the rights of the data subject, the possibility of information and assistance 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 43

Right of access to, rectification, completion, erasure and restriction of the processing of personal data

1. For the purposes laid down in Article 1(1)(a), (b)***,*** and (c) of this Regulation, the data subject's rights of access, rectification, completion, erasure and restriction of the processing shall be exercised in accordance with Chapter III of Regulation (EU) 2016/679 and applied as set out in this Article.

2. The right of access of the data subject in each Member State shall include the right to obtain communication of the data relating to him or her recorded in ***Eurodac, including any record that the person could pose a threat to internal security,*** and of the Member State which transmitted them to ***Eurodac, under*** the ***conditions set out in Regulation (EU) 2016/679 [GDPR] and national law adopted pursuant thereto***. Such access to data ***may*** be granted only by a Member State.

If the rights of rectification and erasure are exercised in a Member State other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of the Member State or States which transmitted the data so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in ***Eurodac.***

3. With regards to the record that the person could pose a threat to internal security, Member States may restrict the data subject's rights referred to in this Article in accordance with Article 23 of Regulation (EU) 2016/679 [GDPR].

4. If it emerges that data recorded in ***Eurodac*** are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall rectify or erase the data in accordance with Article 40(3). That Member State shall confirm in writing to the data subject that it has taken action to rectify, complete, erase or restrict the processing of personal data relating to him or her.

5. If the Member State which transmitted the data does not agree that data recorded in ***Eurodac*** are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject why it is not prepared to rectify 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.

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

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

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

9. The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall, where requested, provide information to the data subject concerning the exercise of his or her right to request from the data controller access, rectification, completion, erasure or restriction of the processing of personal data concerning him or her. The supervisory authorities shall cooperate in accordance with Chapter VII of Regulation (EU) 2016/679.

Article 44

Supervision by the national supervisory authorities

1. Each Member State shall provide that the national supervisory authority or authorities of each Member State referred to in Article ***51(1***) of Regulation (EU) 2016/679 shall monitor the lawfulness of the processing of personal data by the Member State in question for the purposes laid out in Article 1(1)(a), (b) and (c), including their transmission to ***Eurodac***.

2. Each Member State shall ensure that its national supervisory authority has access to advice from persons with sufficient knowledge of biometric data.

Article 45

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning Eurodac, in particular by eu-LISA, are carried out in accordance with Regulation (EC) No 45/2001 and with this Regulation.

2. The European Data Protection Supervisor shall ensure that an audit of the eu-LISA's personal data processing activities is carried out in accordance with international auditing standards at least every three years. A report of such audit shall be sent to the European Parliament, the Council, the Commission, eu-LISA, and the national supervisory authorities. eu-LISA shall be given an opportunity to make comments before the report is adopted.

Article 46

Cooperation between national supervisory authorities and the European Data Protection Supervisor

1. ***In accordance with Article 62 of Regulation (EU) 2018/1725, 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 ***the*** coordinated supervision of Eurodac.

2. Member States shall ensure that every year an audit of the processing of personal data for the purposes laid down in Article 1(1)(e) is carried out by an independent body, in accordance with Article 47(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 57(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 ***within the framework of the European Data Protection Board***. The costs and servicing of these meetings shall be for the account of the European Data Protection ***Board***. 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 ***by the European Data Protection Board*** to the European Parliament, the Council ***and*** the Commission ▌ every two years. This report shall include a chapter of each Member State prepared by the National Supervisory Authority of that Member State.

Article 47

Protection of personal data for law enforcement purposes

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

2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Regulation (EU) 2016/794 and shall be supervised by the European Data Protection Supervisor.

3. Personal data obtained pursuant to this Regulation from Eurodac for the purposes laid down in Article 1(1)(e) shall only be processed for the purposes of the prevention, detection or investigation of the specific case for which the data have been requested by a Member State or by Europol.

4. Without prejudice to Article 24 of Directive (EU) 2016/680, ***Eurodac***, 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 57(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 48

Data security

1. The Member State of origin shall ensure the security of the data before and during transmission to ***Eurodac***.

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 data security plan, in order to:

(a) physically protect the data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing equipment and national installations in which the Member State carries out operations in accordance with the purposes of Eurodac (equipment, access control and checks at entrance to the installation);

(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or erasure of stored personal data (storage control);

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

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

(g) ensure that persons authorised to access Eurodac have access only to the data covered by their access authorisation, by means of individual and unique user IDs and confidential access modes only (data access control);

(h) ensure that all authorities with a right of access to Eurodac create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data, and make those profiles and any other relevant information which those authorities may require for supervisory purposes available to the national supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 and in Article 41 of Directive (EU) 2016/680 without delay at their request (personnel profiles);

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

(j) ensure that it is possible to verify and establish what data have been processed in Eurodac, when, by whom and for what purpose (control of data recording);

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

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

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

(n) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring in order to ensure compliance with this Regulation (self-auditing) and to automatically detect within 24 hours any relevant events arising from the application of measures listed in points (b) to (k) that might indicate the occurrence of a security incident.

3. Member States and Europol shall inform eu-LISA of security incidents detected on their systems related to Eurodac without prejudice to the notification and communication of a personal data breach, pursuant to Articles 33 and 34 of Regulation (EU) 2016/679 and Articles 30 and 31 of Directive (EU) 2016/680, as well as 34 and 35 of Regulation (EU) 2016/794 respectively. Eu-LISA shall inform without undue delay the Member States, Europol and the European Data Protection Supervisor in case of security incidents detected on their systems related to Eurodac without prejudice to Articles 37 and 38 of Regulation (EC) No 45/2001. The Member States concerned, eu-LISA and Europol shall collaborate during a security incident.

4. eu-LISA shall take the necessary measures in order to achieve the objectives set out in paragraph 2 as regards the operation of Eurodac, including the adoption of a data security plan.

Prior to the start of the operational use of Eurodac, the security framework for the Eurodac's business and technical environment shall be updated, in accordance with Article 33 of Regulation (EU) 2018/1725 of the European Parliament and of the Council[24].

[24] ***Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).***

5. ***The*** European Union Agency for Asylum ▌ shall take necessary measures in order to implement Article 18(***4***) of this Regulation, including the adoption of a data security plan referred to in paragraph 2.

Article 49

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 ***Eurodac*** 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 4(2) of Regulation (EU) 2016/679 and Article 3(2) of Directive (EU) 2016/680.

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

3. Personal data which originated in a Member State and are exchanged between a Member State and Europol following a hit obtained for the purposes laid down in Article 1(1)(e) shall not be transferred to third countries if there is a real risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights. In addition, any transfers shall only be carried out when they are necessary and proportionate in cases falling within Europol's mandate, in accordance with Chapter V of Regulation (EU) 2016/794 and subject to the consent of the Member State of origin.

4. No information regarding the fact that an application for international protection has been made or that the person has been subject to an admission procedure in a Member State shall be disclosed to any third-country for persons related to ***Article*** 15(1), ***Article 18*** or ***Article*** 20.

5. 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) 2016/679 or with the national rules adopted pursuant to Chapter V of Directive (EU) 2016/680, as appropriate, to third countries to which Regulation (EU) …/… [▌ Asylum and Migration Management ***Regulation***] applies.

Article 50

Transfer of data to third countries for the purpose of return

1. By way of derogation from Article 49 of this Regulation, the personal data relating to persons referred to in Articles 15(1), 22(2), 23(1) ***and 24(1)*** obtained by a Member State following a hit for the purposes laid down in Article 1(1)(a) or (***c***) may be transferred or made available to a third-country with the agreement of the Member State of origin.

2. The transfer of the data to a third country shall be carried out in accordance with the relevant provisions of Union law, in particular provisions on data protection, including Chapter V of Regulation (EU) 2016/679, and, where applicable, readmission agreements, and the national law of the Member State transferring the data.

3. The transfers of data to a third country shall take place only when the following conditions are met:

   (a) the data is transferred or made available solely for the purpose of identification of, and issuance of an identification or travel document to, an illegally staying third-country national in view of return;

   (b) the third-country national concerned has been informed that his or her personal data may be shared with the authorities of a third country.

4. Implementation of Regulation (EU) 2016/679, including with regard to the transfer of personal data to third countries pursuant to this Article, and in particular the use, proportionality and necessity of transfers based on Article 49(1)(d) of that Regulation, shall be subject to monitoring by the national independent supervisory authority set up pursuant to Chapter VI of Regulation (EU) 2016/679.

5. Transfers of personal data to third countries pursuant to this Article shall not prejudice the rights of persons referred to in Article 15(1), 18(1) and 20***(1)*** of this Regulation, in particular as regards non-refoulement, and the prohibition to disclose or obtain information in accordance with Article ***8*** of Regulation (EU) …/… [Asylum Procedure Regulation].

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

Article 51

Logging and documentation

1. Each Member State and Europol shall ensure that all data processing operations resulting from requests for comparison with Eurodac data for the purposes laid down in Article 1(1)(***c***) are logged or documented for the purposes of checking the admissibility of the request, monitoring the lawfulness of the data processing and data integrity and security, and self-monitoring.

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 33(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 ***Eurodac***;

(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 32(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 Regulation (EU) 2016/794, the identifying mark of the official who carried out the search and of the official who ordered the search or supply;

(i) where ***applicable*** a reference to the use of the European search portal to query ▌ Eurodac as referred to in Article 7(2) of the Regulation ***(EU)*** 2019/818.

3. Logs and documentation shall be used only for monitoring the lawfulness of data processing and for ensuring data integrity and security. Only logs which do not contain personal data may be used for the monitoring and evaluation referred to in Article 57.

The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data processing and data integrity and security shall have access to these logs at their request for the purpose of fulfilling their tasks.

Article 52

Liability

1. Any person who, or Member State which, has suffered material or non-material damage as a result of an unlawful processing operation or any other act incompatible with this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered or from eu-LISA if it is responsible for the damage suffered only where it has not complied with obligations on it pursuant to this Regulation specifically directed to it or where it has acted outside or contrary to lawful instructions of that Member State. That Member State or eu-LISA 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 any failure of a Member State to comply with its obligations under this Regulation causes damage to ***Eurodac***, that Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State failed to take reasonable steps to prevent the damage from occurring or to minimise its impact**.**

3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State in accordance with Articles 79 and 80 of Regulation (EU) 2016/679 and Articles 54 and 55 of Directive (EU) 2016/680. Claims for compensation against eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for by the Treaties.

Chapter XIII

Amendments to Regulations (EU) 2018/1240, (EU) 2019/818

Article 53

Amendments to Regulation (EU) 2018/1240

(1) in Article 11 the following paragraph 6a is inserted:

‘6a. For the purpose of proceeding to the verifications referred to in point (k) of Article 20(2), the automated processing referred to in paragraph 1 of this Article, shall enable the ETIAS Central System to query Eurodac established by [Regulation (EU) …/…], with the ▌ data ***referred to in*** Article 17(2)***, points*** (a) to (d):

(a) surname (family name), surname at birth, first name(s) (given name(s)), date of birth, place of birth, sex, current nationality;

(b) other names (alias(es), artistic name(s), usual name(s)) if any;

(c) other nationalities (if any);

(d) type, number, the country of issue of the travel document.’;

(2) in Article 25a(1) ***the following*** point (e) is ***inserted***:

‘(***f***) ***data referred to in*** Articles 17***, 19, 21***, 22, 23***, 24*** and 26 of Regulation (EU) …/… [Eurodac Regulation].’;

(3) in Article 88, paragraph 6 is replaced by the following:

‘6. ETIAS’ operations shall start irrespective of whether interoperability with Eurodac or ECRIS-TCN is put in place.’.

Article 54

Amendments to Regulation (EU) 2019/818

Regulation (EU 2019/818 is amended as follows:

(1) in Article 4, point (20) is replaced by the following:

‘(20) “designated authorities” means the Member State designated authorities as defined in Article 7 of Regulation (EU) …/… [Eurodac Regulation], in point (26) of Article 3(1) of Regulation (EU) 2017/2226 of the European Parliament and the Council, in point (3a) of Article 4 of Regulation (EC) No 767/2008, and point (21) of Article 3(1) of Regulation (EU) 2018/1240 of the European Parliament and of the Council ▌ ’;

(2) in paragraph 1 of Article 10, the introductory wording is replaced by the following:

‘Without prejudice to Article 51 of Regulation (EU) …/… [Eurodac Regulation], Articles 12 and 18 of Regulation (EU) 2018/1862, Article 29 of Regulation (EU) 2019/816 and Article 40 of Regulation (EU) 2016/794, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:’;

(3) paragraph 1 of Article 13 is amended as follows:

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

‘(b) the data referred to in Article 5(1), point (b), and (***3***) of Regulation (EU) 2019/816;’;

(b) the following point (c) is added:

‘(c) the data referred to in Articles 17(1), points (a) and (b), 19***,*** points (a) and (b), 21 ▌ points (a) and (b), 22(2), points (a) and (b), 23(2), points (a) and (b) ▌***,*** 24***(2), points (a) and (b) and 26***(2), points (a) and (b) of Regulation (EU) …/ [Eurodac Regulation].’;

(4) Article 14 is replaced by the following:

‘Article 14
Searching biometric data with the shared biometric matching service

In order to search the biometric data stored within the CIR and SIS, the CIR and SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in Regulations (EC) No 767/2008, (EU) 2017/2226, Regulation (EU) …/… [Eurodac Regulation], Regulations (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 and (EU) 2019/816.’;

(5) In Article 16, the introductory wording of paragraph 1 is replaced by the following:

‘Without prejudice to Article 51 of Regulation (EU) … [Eurodac Regulation], Article 12 and 18 of Regulation (EU) 2018/1862 and to Article 29 of Regulation (EU) 2019/816, eu-LISA shall keep logs of all data processing operations within the shared BMS.’;

(6) In Article 18, paragraph 1 is replaced by the following:

‘1. The CIR shall store the following data, logically separated according to the information system from which the data have originated:

(a) the data referred to in Article 17(1), points (a) to (f), (h) and (i), ***Article 19 points (a) to (f***), (h) and (i), Article 21 points (a) to (f), (h) and (i), Article 22(2), points (a) to (f), (h) and (i), Article 23(2), points (a) to (f), (h) and (i) ▌**,** Article 24***(2), points (a) to (f) and (h) and (3) point (a) and Article 26(2)***, points (a) to (f), (h) and (i) of Regulation (EU) …/… [Eurodac Regulation];

(b) the data referred to in Article 5(1), point (b), and (***3***) and the following data listed in Article 5(1), point (a) of Regulation (EU) 2019/816: surname (family name), first names (given names), date of birth, place of birth (town and country), nationality or nationalities, gender, previous names, if applicable, where available pseudonyms or aliases, as well as, where available, information on travel documents.';

(7) in Article 23, paragraph 1 is replaced by the following:

'1. The data referred to in Article 18(1), (2) and (2a) shall be deleted from the CIR in an automated manner in accordance with the data retention provisions of Regulation (EU) …/… [Eurodac Regulation] and of Regulation (EU) 2019/816.';

(8) Article ***24(1)***, is replaced by the following:

'Article 24
Keeping of logs

Without prejudice to Article 51 of Regulation (EU) …/… [Eurodac Regulation] and Article 29 of Regulation (EU) 2019/816, eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4 of this Article.';

(9) in Article 26(1), points (aa)***, (aaa)***, (ab), (ac) ▌**,** (ad) ***and (ae)*** are inserted:

‘(aa) the authorities competent to ***collect the data provided for in Chapter II of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac;***

(aaa) the authorities competent to collect the data provided for in Chapter III of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac for matches that occurred when transmitting such data;

(ab) the authorities competent to collect the data provided for in Chapter IV of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac;

(ac) the authorities competent to collect the data provided for in Chapter V of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac;

(ad) the authorities competent to collect the data provided for in Chapter VI of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac;

(ae) the authorities competent to collect ***the*** data provided for in Chapter VIII of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac;’;

(10) Article 27 is amended as follows:

(a) the following point (aa) is inserted in paragraph 1:

‘(aa) a data set is transmitted to Eurodac in accordance with Articles 17, 19, 21, 22, 23***, 24*** and 26 of Regulation (EU) …/… [Eurodac Regulation];’;

(b) the following point (aa) is inserted in paragraph 3:

‘(aa) surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 17 ▌***, 19, 21, 22, 23,*** 24 ***and 26*** of Regulation (EU) …/… [Eurodac Regulation];’;

(11) in Article 29(1), the following ***points*** (aa)***, (aaa), (ab), (ac), (ad) and (ae) are*** inserted:

‘(aa) the ***authorities competent to collect the data provided for in Chapter II of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac for matches that occurred when transmitting such data;***

(aaa) the authorities competent to collect the data provided for in Chapter III of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac for matches that occurred when transmitting such data;

(ab) the authorities competent to collect the data provided for in Chapter IV of Regulation (EU) …/… [Eurodac Regulation] for matches that occurred when transmitting such data;

(ac) the authorities competent to collect the data provided for in Chapter V of Regulation (EU) …/… [Eurodac Regulation] for matches that occurred when transmitting such data;

(ad) the authorities competent to collect the data provided for in ***Chapter VI of*** Regulation (EU) …/… [Eurodac Regulation] ***when transmitting data to Eurodac*** for ***matches*** that occurred when ***transmitting*** such ***data***;

(ae) the authorities competent to collect the data provided for in Chapter VIII of Regulation (EU) …/… [Eurodac Regulation] when transmitting data to Eurodac for matches that occurred when transmitting such data.';

(12) in Article 39, paragraph 2 is replaced by the following:

‘2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in ***Article 14*** of Regulation (EU) …/… [Eurodac Regulation], Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816 logically separated by EU information system. Access to the repository CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in ***Article 14*** of Regulation (EU) …/… [Eurodac Regulation], Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816.’;

(13) in Article 47, the following new indent is inserted in paragraph 3:

‘Persons whose data are recorded in the Eurodac shall be informed about the processing of personal data for the purposes of this Regulation in accordance with paragraph 1 when a new data set is transmitted to Eurodac in accordance with Articles 15, 18, 20, 22, 23***, 24*** and 26 of Regulation (EU) …/… [Eurodac Regulation].’;

(14) Article 50 is replaced by the following:

‘Article 50

Communication of personal data to third countries, international organisations and private parties

Without prejudice to Article 31 of Regulation (EC) No 767/2008, Articles 25 and 26 of Regulation (EU) 2016/794, Articles 49 and 50 of Regulation (EU) …/… [Eurodac Regulation], Article 41 of Regulation (EU) 2017/2226, Article 65 of Regulation (EU) 2018/1240 and the querying of Interpol databases through the ESP in accordance with Article 9(5) of this Regulation which comply with the provisions of Chapter V of Regulation (EU) 2018/1725 and Chapter V of Regulation (EU) 2016/679, personal data stored in, processed or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party.’.

Chapter XIV
Final provisions

Article 55
Costs

1. The costs incurred in connection with the establishment and operation of ***Eurodac*** 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 Europol access point and their costs for connection to the ***Eurodac*** shall be borne by each Member State and Europol respectively.

3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and shall be responsible for bearing its costs resulting from requests for comparison with Eurodac data for the purposes laid down in Article 1(1)(e).

Article 56

Committee Procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where the Committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 57

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 ***Eurodac***, 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 ***Eurodac*** 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 ***Eurodac***.

4. ***Within*** three years ***from the entry into force of this Regulation,*** eu-LISA shall conduct a study on the technical feasibility of adding facial recognition software to ***Eurodac*** for the purposes of comparing facial images, including of minors. 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 ***Eurodac***.

5. By … [***three*** years ***from the date of application of this Regulation***] 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, in particular data protection and privacy 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 including the use of facial recognition software, and any implications for future operations, and shall make any necessary recommendations. This evaluation shall also include an assessment of the synergies between this Regulation and the Regulation (EU) 2018/1862 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters. The Commission shall transmit the evaluation to the European Parliament and the Council.

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

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

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

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

– grounds given for reasonable suspicion,

– the reasonable grounds given not to conduct comparison with other Member States under Decision 2008/615/JHA, in accordance with Article 33(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 reports shall be transmitted to the Commission by 30 June of the subsequent year.

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

Article 58

Assessment

1. By … [48 months from the date of entry into force of this Regulation], the Commission shall assess the functioning and the operational efficiency of any IT system used to exchange the data of the beneficiaries of temporary protection for the purposes of the administrative cooperation referred to in Article 27 of Council Directive 2001/55/EC.

2. The Commission shall also assess the expected impact of applying Article 26 of the present Regulation in case of a future activation of Council Directive 2001/55/EC, taking into consideration:

(a) the nature of data subject to processing,

(b) the expected impact of providing access to the data listed in Article 26(2) to the designated authorities referred to in Articles 7(1) and 9(1),

(c) the safeguards provided for in the Regulation.

3. Depending on the outcome of the assessments referred to in paragraphs 1 and 2, the Commission shall make a legislative proposal amending or repealing Article 26, if appropriate.

Article 59

Penalties

Member States shall take the necessary measures to ensure that any processing of data entered in ***Eurodac*** 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 60

Territorial scope

The provisions of this Regulation shall not be applicable to any territory to which Regulation (EU) …/… [Asylum and Migration Management Regulation] does not apply, with the exception of the provisions related to data collected to assist with the application of Regulation (EU) …/… [Resettlement Regulation] under the conditions set out in this Regulation

Article 61

Notification of designated authorities and verifying authorities

1. By … [***three months from the date of entry into force of this Regulation***], each Member State shall notify the Commission of its designated authorities, of the operating units referred to in Article 8(3) and of its verifying authority ▌ and shall notify without delay any amendment thereto.

2. By … [***three months from the date of entry into force of this Regulation***], Europol shall notify the Commission of its designated authority and of its verifying authority ▌ 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 62

Repeal

Regulation (EU) No 603/2013 is repealed with effect from … [***24 months from the date of entry into force of this Regulation***].

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

Article 63

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

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

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 ***Eurodac***. Facial recognition software shall be introduced into ***Eurodac*** within one year from the conclusion of the study on the introduction of facial recognition software referred to in Article 57(4). Until that day, facial images shall be stored in ***Eurodac*** as part of the data-subject's data sets and transmitted to a Member State following the comparison of fingerprints where there is a hit result.

Member States shall notify the Commission and eu-LISA as soon as they have made the technical arrangements to transmit data to ***Eurodac***, no later than [date of application of this Regulation].

Article 26 shall apply as from three years after the entry into application of the other provisions.

This Regulation shall not apply to those persons benefiting from temporary protection pursuant to Council Implementing Decision (EU) 2022/382, and any other equivalent national protection taken pursuant thereto, any future amendments to Council Implementing Decision (EU) 2022/382, and any extensions thereto.

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*

ANNEX I

Table of correspondences referred to in Article 10

Data provided pursuant to Article 17(2) of Regulation (EU) 2018/1240 of the European Parliament and of the Council[1] recorded and stored by ETIAS Central System	The corresponding data in Eurodac pursuant to Articles 17, 19***, 21, 22***, 23***, 24 and 26*** of this Regulation against which the ETIAS data should be checked
surname (family name)	surname(s)
surname at birth	name(s) at birth
first name(s) (given name(s))	forename(s)
other names (alias(es), artistic name(s), usual name(s))	previously used names and any aliases
date of birth	date of birth
place of birth	place of birth
sex	sex
current nationality	nationality(ies)
other nationalities (if any)	nationality(ies)
type of the travel document	type of travel document
number of the travel document	number of travel document
country of issue of the travel document	three letter code of the issuing country

[1] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

ANNEX II

Correlation Table

[…]