


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

Commission proposal (doc. 8765/1/16 REV 1)	EP position	Council's mandate for negotiations with the EP (doc. 10079/17)	
Proposal for a	Draft European Parliament legislative resolution	Draft	
<p>REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ☒ , for identifying an illegally staying third-country national or stateless person ☒ and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the</p>	<p>Amendment 1 REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, <i>and amending Regulation (EU) No 1077/2011 (recast)</i></p>	<p>REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of <u>biometric data</u> [...] for the effective application of [Regulation (EU) No <u>XXX/XXX</u> <u>[Dublin Regulation]</u> [...] establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, <u>and amending Regulation (EU) No 1077/2011</u> [...] (recast)</p>	

area of freedom, security and justice (recast)			
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	
Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 78 (2)(e), <input checked="" type="checkbox"/> 79(2)(c), <input checked="" type="checkbox"/> 87(2)(a) and 88(2)(a) thereof,	Amendment 2 Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 78 (2)(d) and (e) , 79(2)(c), 87(2)(a) and 88(2)(a) thereof,		
Having regard to the proposal from the European Commission			
After transmission of the draft legislative act to the national Parliaments,			
		Having regard to the opinion of the European Economic and Social Committee,	
Having regard to the opinion of the European Data Protection Supervisor,			
Acting in accordance with the ordinary legislative procedure,			
Whereas:		Whereas:	
(1) A number of substantive changes are to be made to Council			

<p>Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention¹ and to Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention² <input checked="" type="checkbox"/> Regulation (EU) No 603/2013 of the European Parliament and of the Council³ <input checked="" type="checkbox"/> . In the interests of clarity, those <input checked="" type="checkbox"/> that <input checked="" type="checkbox"/> Regulations should be recast.</p>			
<p>(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom,</p>			

¹ ~~OJ L 316, 15.12.2000, p. 1.~~

² ~~OJ L 62, 5.3.2002, p. 1.~~

³ Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).

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

PUBLIC

<p>(4) For the purposes of applying Regulation (EU) No [...] of the European Parliament and of the Council⁴ of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person⁵, it is necessary to establish the identity of applicants for international protection and of persons apprehended in connection with the unlawful crossing of the external borders of the Union. It is also desirable, in order effectively to apply Regulation (EU) No [.../...], and in particular Articles[...] and [..] thereof, to allow each Member State to check whether a third-country national or stateless person found illegally staying on its territory has applied for international protection in another Member State.</p>		<p>(4) For the purposes of applying Regulation (EU) No XXX/XXX [Dublin Regulation] [...] establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, it is necessary to establish the identity of applicants for international protection and of persons apprehended in connection with the unlawful crossing of the external borders of the Union. It is also desirable, in order effectively to apply Regulation (EU) No XXX/XXX [Dublin Regulation] [...], and in particular Articles [...] and [...]) thereof, to allow each Member State to check whether a third-country national or stateless person found illegally staying on its territory has applied for international protection in another Member State.</p>	
---	--	--	--

⁴ ~~Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person (OJ L 180, 29.6.2013, p. 31).~~

⁵ See page 31 of this Official Journal.

	<p>Amendment 3</p> <p><i>(4a) It is necessary that all Member States register in Eurodac information on resettled third-country nationals and stateless persons for the purposes of identifying secondary movements of such persons.</i></p>		
	<p>Amendment 4</p> <p><i>(4b) The registration in Eurodac of information on resettled third-country nationals or stateless persons is designed to ensure that such persons enjoy, in accordance with [Regulation XXX/XXX], the same level of protection and the same rights applicable to other beneficiaries of international protection as regards the processing of their data. This should also enable Member States to verify whether or not a third-country national or stateless person has already been resettled in another Member State in accordance with Regulation XXX/XXX. Where a third-country national or stateless person has already been resettled, it should be possible to establish the Member State of resettlement</i></p>		

	<i>and to monitor any secondary movements.</i>		
<p>(5) Fingerprints ⇒ Biometrics ⇐ constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint ⇐ and facial image ⇐ data.</p>	<p>Amendment 5</p> <p>(5) Biometrics constitute an important element in establishing the exact identity of such persons <i>because they ensure high accuracy of identification.</i> It is necessary to set up a system for the comparison of their <i>biometric</i> data.</p>	<p>(5) Biometrics constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their biometric [...] data.</p>	
<p>(6) To that end, it is necessary to set up a system known as 'Eurodac', consisting of a Central System, which will operate a computerised central database of fingerprint ⇐ and facial image ⇐ data, as well as of the electronic means of transmission between the Member States and the Central System, hereinafter the "Communication Infrastructure".</p>		<p>(6) To that end, it is necessary to set up a system known as 'Eurodac', consisting of a Central System, which will operate a computerised central database of biometric [...] data, as well as of the electronic means of transmission between the Member States and the Central System, hereinafter the "Communication Infrastructure".</p>	

<p>(7) For the purposes of applying and implementing Regulation (EU) No. [...] it is also necessary to ensure that a separate secure communication infrastructure exists, which Member State's competent authorities for asylum can use for the exchange of information on applicants for international protection. This secure electronic means of transmission shall be known as 'DubliNet' and should be managed and operated by eu-LISA.</p>		<p>(7) For the purposes of applying and implementing Regulation (EU) No. XXX/XXX [Dublin Regulation] [...] it is also necessary to ensure that a separate secure communication infrastructure exists, which Member State's competent authorities for asylum can use for the exchange of information on applicants for international protection. The DubliNet network established by Commission Regulation (EC) 1560/2003⁶ ('DubliNet') should be such_[...] secure electronic means of transmission [...], and it should be managed and operated by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council⁷ ("eu-LISA"). It is also necessary to modify the Regulation (EU) No. 1077/2011</p>	
--	--	---	--


⁶ Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ L 222, 5.9.2003, p. 3).

⁷ Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p. 1).

		in order to reflect this new task entrusted to eu-LISA.	
<p>(8) The Hague Programme called for the improvement of access to existing data filing systems in the Union. In addition, The Stockholm Programme called for well-targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.</p>			
<p>(9) In 2015, the refugee and migration crisis brought to the fore challenges faced by some Member States with taking fingerprints of illegally staying third-country nationals or stateless persons who attempted to avoid the procedures for determining the Member State responsible for examining an application for international protection. The Communication of the Commission of 13 May 2015, titled "A European Agenda on Migration"⁸ noted that "<i>Member States must also implement fully the rules on taking migrants' fingerprints at the borders</i>" and further proposed that "<i>The Commission will also explore how</i></p>	<p>Amendment 6</p> <p>(9) In 2015, the refugee and migration crisis brought to the fore challenges faced by some Member States with taking fingerprints of illegally staying third-country nationals or stateless persons who attempted to avoid the procedures for determining the Member State responsible for examining an application for international protection.The Communication of the Commission of 13 May 2015, titled "A European Agenda on Migration"²⁵ noted that "Member States must also implement fully the rules on taking migrants' fingerprints at the borders" and further proposed that "the</p>		

⁸ COM(2015) 240 final, 13.5.2015

<p><i>more biometric identifiers can be used through the Eurodac system (such as using facial recognition techniques through digital photos)".</i></p>	<p>Commission will also explore how more biometric identifiers can be used through the Eurodac system (such as using facial recognition techniques through digital photos)".</p>		
<p>(10) To assist Member States overcome challenges relating to non-compliance with the fingerprinting process, this Regulation also permits the comparison of a facial image without fingerprints as a last resort, where it is impossible to take the fingerprints of the third-country national or stateless person because his or her fingertips are damaged, either intentionally or not, or amputated. Member States should exhaust all attempts to ensure that fingerprints can be taken from the data-subject before a comparison using a facial image only can be carried out where non-compliance based on reasons not relating to the conditions of the individual's fingertips are given. Where facial images are used in combination with fingerprint data, it allows for the reduction of fingerprints registered while enabling the same result in terms of accuracy of the</p>	<p>Amendment 7</p> <p>(10) To assist Member States overcome challenges relating to non-compliance with the fingerprinting process, this Regulation also permits the comparison of a facial image without fingerprints as a last resort, where it is impossible to take the fingerprints of the third-country national or stateless person because his or her fingertips are damaged, either intentionally or not, or amputated.</p> <p><i>For the purposes of obtaining high accuracy identification, fingerprints should always be preferred over facial images.</i></p> <p>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. <i>To assist Member States overcome challenges, where it is impossible to take the fingerprints of the</i></p>	<p>(10) To assist Member States overcome challenges [...], where it is impossible to take the fingerprints of the third-country national or stateless person because his or her fingertips are damaged, either intentionally or not, or amputated, this Regulation also permits the comparison of a facial image without fingerprints. Member States should exhaust all attempts to ensure that fingerprints can be taken from the data-subject before a comparison using a facial image only can be carried out [...].</p>	

<p>identification.</p>	<p><i>third-country national or stateless person because his or her fingertips are damaged, either intentionally or not, or amputated, this Regulation should also permit the comparison of a facial image without fingerprints.</i> where non-compliance based on reasons not relating to the conditions of the individual's fingertips are given. Where facial images are used in combination with fingerprint data, it allows for the reduction of fingerprints registered while enabling the same result in terms of accuracy of the identification. Where <i>the physical impossibility to give fingerprints is of a temporary nature, that fact should be recorded and the fingerprinting process should be carried out at a later stage when the physical integrity of the fingertips is restored.</i></p>		
------------------------	--	---	--

<p>(11) The return of third-country nationals who do not have a right to stay in the Union, in accordance with fundamental rights as general principles of Union law as well as international law, including refugee protection and human rights obligations, and in compliance with the provisions of Directive 2008/115/EC⁹, is an essential part of the comprehensive efforts to address migration and, in particular, to reduce and deter irregular migration. To increase the effectiveness of the Union system to return illegally staying third-country nationals is needed in order to maintain public trust in the Union migration and asylum system, and should go hand in hand with the efforts to protect those in need of protection.</p>	<p>Amendment 8</p> <p>(11) The return of third-country nationals <i>or stateless persons</i> 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, <i>the principle of non-refoulement</i> and human rights obligations, and in compliance with the provisions of Directive 2008/115/EC¹⁰, is an essential <i>important</i> part of the comprehensive efforts to address migration <i>in a fair and efficient way</i> and, in particular, to reduce and deter irregular migration. To increase the effectiveness of the Union system to return illegally staying third-country nationals <i>or stateless persons</i> 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</p>	<p>(11) The return of third-country nationals or stateless persons who do not have a right to stay in the Union, in accordance with fundamental rights as general principles of Union law as well as international law, including refugee protection and human rights obligations, and in compliance with the provisions of Directive 2008/115/EC¹¹, is an essential part of the comprehensive efforts to address migration and, in particular, to reduce and deter irregular migration. To increase the effectiveness of the Union system to return illegally staying third-country nationals or stateless persons is needed in order to maintain public trust in the Union migration and asylum system, and should go hand in hand with the efforts to protect those in need of protection.</p>	
---	--	--	--

⁹ Directive of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24.12.2008, p. 98.

¹⁰ Directive of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24.12.2008, p. 98.

¹¹ Directive of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ L 348, 24.12.2008, p. 98.

	those in need of protection.		
<p>(12) National authorities in the Member States experience difficulties in identifying illegally staying third-country nationals who use deceptive means to avoid their identification and to frustrate the procedures for re-documentation in view of their return and readmission. It is therefore essential to ensure that information on third-country nationals or stateless persons who are found to be staying illegally in the EU are collected and transmitted to Eurodac and are compared also with those collected and transmitted for the purpose of establishing the identity of applicants for international protection and of third-country nationals apprehended in connection with the unlawful crossing of the external borders of the Union, in order to facilitate their identification and re-documentation and to ensure their return and readmission, and to reduce identity fraud. It should also contribute to reducing the length of the administrative procedures necessary for ensuring return and readmission of illegally</p>	<p>Amendment 9</p> <p>(12) National authorities in the Member States experience difficulties in identifying illegally staying third-country nationals who use deceptive means to avoid their identification and to frustrate the procedures for re-documentation 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 found to be staying illegally in the <i>Union</i> are collected and transmitted to Eurodac and are compared also with those collected and transmitted for the purpose of establishing the identity of applicants for international protection and of third-country nationals or stateless persons apprehended in connection with the unlawful crossing of the external borders of the Union, in order to facilitate their identification and re-documentation and to ensure their return and readmission, and to reduce identity fraud. It should</p>	<p>(12) National authorities in the Member States experience difficulties in identifying illegally staying third-country nationals or stateless persons who use deceptive means to avoid their identification and to frustrate the procedures for re-documentation in view of their return and readmission. It is therefore essential to ensure that information on third-country nationals or stateless persons who are found to be staying illegally in the EU are collected and transmitted to Eurodac and are compared also with those collected and transmitted for the purpose of establishing the identity of applicants for international protection and of third-country nationals or stateless persons apprehended in connection with the unlawful crossing of the external borders of the Union, in order to facilitate their identification and re-documentation and to ensure their return and readmission, and to reduce identity fraud. It should also contribute to reducing the length of the administrative</p>	

staying third-country nationals, including the period during which they may be kept in administrative detention awaiting removal. It should also allow identifying third countries of transit, where the illegally staying third-country national may be readmitted.	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. <i>This should be without prejudice to the operation and use of the Schengen Information System (SIS), which remains the primary system to ensure cooperation and information exchange on return.</i>	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.	
	Amendment 10 <i>(12a) Member States should be able to derogate from the provisions of Article 14 in respect of illegally staying third-country nationals who entered the Union by legally crossing the external border where they have overstayed their authorised period of stay by a period of no more than 15 days.</i>		
		(12a) With a view to facilitating	


		<p>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 the Central System 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 the Central System along with an indication of its authenticity.</p> <p>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.</p>	
--	--	---	--

<p>(13) In its Conclusions of 8 October 2015 on the future of return policy, the Council endorsed the initiative announced by the Commission to explore an extension of the scope and purpose of Eurodac to enable the use of data for return purposes¹². Member States should have the necessary tools at their disposal to be able to detect illegal migration to and secondary movements of illegally staying third-country nationals in the Union. Therefore, the data in Eurodac should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of the Member States.</p>	<p>Amendment 11</p> <p>(13) In its Conclusions of 8 October 2015 on the future of return policy, the Council endorsed the initiative announced by the Commission to explore an extension of the scope and purpose of Eurodac to enable the use of data for return purposes¹³. Member States should have the necessary tools at their disposal to be able to detect illegal migration to <i>the Union and to identify</i> secondary movements and illegally staying third-country nationals <i>and stateless persons</i> 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.</p>	<p>(13) In its Conclusions of 8 October 2015 on the future of return policy, the Council endorsed the initiative announced by the Commission to explore an extension of the scope and purpose of Eurodac to enable the use of data for return purposes¹⁴. Member States should have the necessary tools at their disposal to be able to detect illegal migration to and secondary movements of illegally staying third-country nationals or stateless persons in the Union. Therefore, the data in Eurodac should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of the Member States.</p>	
--	---	--	--

¹² EU Action Plan on return, COM(2015) 453 final.


¹³ EU Action Plan on return, COM(2015) 453 final.

¹⁴ EU Action Plan on return, COM(2015) 453 final.

	<p>Amendment 12</p> <p><i>(13 a) The European Border and Coast Guard Agency, as established by Regulation (EU) 2016/1624 of the European Parliament and of the Council^{15a}, plays a key role in the Union's efforts for a better management of external borders, and the prevention of illegal immigration and secondary movements. Consequently, the European Border and Coast Guard Agency should be provided with access to Eurodac data in order to be able to undertake risk analyses to the highest possible standard and to assist Member States with return-related tasks. Those data should be processed in compliance with the data protection safeguards provided for in that Regulation.</i></p>		<p><i>Confirmed by trilogue (link to EP amendments 70, 75 and 77)</i></p> <p><i>(13 a) The European Border and Coast Guard Agency, as established by Regulation (EU) 2016/1624 of the European Parliament and of the Council[1]a, 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.</i></p>
--	--	---	--

¹⁵

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

	<p>Amendment 13</p> <p><i>(13 b) As one of the tasks of the European Border and Coast Guard Agency and the European Union Agency for Asylum, referred to in this Regulation, is the taking and transmitting of biometric data, the European Border and Coast Guard Agency and the European Union Agency for Asylum should be provided with their own interfaces so that they no longer need to rely on national infrastructures. In the long run, those interfaces could be used as a single search interface, as described in the Commission Communication of 6 April 2016 entitled "Stronger and Smarter Information Systems for Borders and Security"¹⁶.</i></p>		<p><i>Confirmed by trilogue (link to EP amendments 70, 75 and 77)</i></p> <p><i>(13 b) 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) XXX/XXX [Regulation on the EU Agency for Asylum] 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.</i></p>
--	--	---	--

<p>(14) The Commission's Communication on Stronger and Smarter Information Systems for Borders and Security¹⁷ highlights the need to improve the interoperability of information systems as a long-term objective, as also identified by the European Council and the Council. The Communication proposes to set up an Expert Group on Information Systems and Interoperability to address the legal and technical feasibility of achieving interoperability of the information systems for borders and security. This group should assess the necessity and proportionality of establishing interoperability with the Schengen Information Systems (SIS) and the Visa Information Systems (VIS), and examine if there is a need to revise the legal framework for law enforcement access to EURODAC.</p>	<p>Amendment 14</p> <p>(14) The Commission's <i>In line with its</i> Communication on Stronger and Smarter Information Systems for Borders and Security¹⁸ highlights, <i>which highlighted</i> the need to improve the interoperability of information systems as a long-term objective, as also identified by the European Council and the Council, The Communication proposes to set <i>the Commission set</i> up an Expert Group on Information Systems and Interoperability to address the legal and technical feasibility of achieving interoperability of the information systems for borders and security. This group should assess the necessity and proportionality of establishing <i>which would allow for simpler and quicker access to all relevant information and for improving the quality of service that the relevant databases provide to their users. Therefore, technological solutions should be developed to ensure the</i></p>	<p>(14) The Commission's Communication on Stronger and Smarter Information Systems for Borders and Security¹⁹ highlights the need to improve the interoperability of information systems as a long-term objective, as also identified by the European Council and the Council. The Communication proposes to set up an Expert Group on Information Systems and Interoperability to address the legal and technical feasibility of achieving interoperability of the information systems for borders and security. This group should assess the necessity and proportionality of establishing interoperability <i>between the various Union information systems [...].</i></p>	
--	---	---	--

¹⁷ COM(2016) 205 final


¹⁸ COM(2016) 0205

¹⁹ COM(2016) 205 final

	<p>interoperability <i>of Eurodac</i> with the Schengen Information Systems (SIS)and, the Visa Information Systems (VIS), and examine if there is a need to revise the legal framework for law enforcement access to Eurodac) <i>Europol</i>, and <i>any new relevant information systems developed in the area of freedom, security and justice, in order to enhance effective cooperation among Member States in managing external borders and combatting serious crime. In particular, an assessment should be made as to whether interoperability should be established between Eurodac and the Entry-Exist-System (EES) in order to allow consultation between the EES and Eurodac of the data of third-country nationals or stateless persons having exceeded the maximum duration of authorised stay.</i></p>		
	<p>Amendment 15</p> <p><i>(14a) Eu-LISA should establish a secure communication channel between the EES central system and the Eurodac central system in order to enable interoperability</i></p>		

	<i>between them. It is necessary to connect the two central systems to allow for the transfer to Eurodac of the biometric data of a third-country national registered in the EES where registration of those biometric data are required by this Regulation.</i>		
--	--	--	--

PUBLIC

<p>(15) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in Eurodac is necessary for the purposes of the prevention, detection or investigation of terrorist offences as referred to in Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism²⁰ or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States²¹. 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</p>	<p>Amendment 16</p> <p>(15) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in Eurodac is necessary for the purposes of the prevention, detection or investigation, investigation or prosecution of terrorist offences as referred to in Directive (EU) 2017/... of the European Parliament and of the Council [combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA]²² or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA²³. Therefore, the data in Eurodac should be available, subject to the conditions set out in this</p>		
---	--	---	--


²⁰ Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

²¹ 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).

²² Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

²³ 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).

Police Office (Europol).	Regulation, for comparison by the designated authorities of Member States and the European Police Office (Europol).		
(16) The powers granted to law enforcement authorities to access Eurodac should be without prejudice to the right of an applicant for international protection to have his or her application processed in due course in accordance with the relevant law. Furthermore, any subsequent follow-up after obtaining a 'hit' from Eurodac should also be without prejudice to that right.			
(17) The Commission outlines outlined in its Communication to the Council and the European Parliament of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs that authorities responsible for internal security could have access to Eurodac in well-defined cases, when there is a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for			


<p>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.</p>			
<p>(18) Moreover, Europol plays a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to Eurodac within the framework of its tasks and in accordance with Council Decision 2009/371/JHA</p>		<p>(18) Moreover, Europol plays a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to Eurodac within the framework of its tasks and in accordance with Regulation (EU) 2016/794 of the</p>	


of 6 April 2009 establishing the European Police Office (Europol) ²⁴ .		European Parliament and of the Council ²⁵ [...].	
(19) Requests for comparison of Eurodac data by Europol should be allowed only in specific cases, under specific circumstances and under strict conditions.	Amendment 17 (19) Requests for comparison of Eurodac data by Europol should be allowed only in specific cases, under specific circumstances and under strict conditions, <i>in line with the principles of necessity and proportionality enshrined in Article 52(1) of the Charter of Fundamental Rights of the European Union and as interpreted by the Court of Justice of the European Union</i> ²⁶ .		
(20) Since Eurodac was originally established to facilitate the application of the Dublin Convention, access to Eurodac for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes a change of the original purpose of Eurodac,	Amendment 18 (20) Since Eurodac was originally established to facilitate the application of the Dublin Convention, access to Eurodac for the purposes of preventing, detecting or investigating, <i>investigating or prosecuting</i> terrorist offences or other serious		

²⁴ Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).

²⁵ **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 [...]**

²⁶ *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.*

<p>which interferes with the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac. ⇒ In line with the requirements of Article 52(1) of the Charter of Fundamental Rights of the European Union, ⇐ Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to protect a legitimate and proportionate ⇒ to genuinely meet an objective of general ⇐ interest and proportionate to the legitimate objective it aims to achieve.</p>	<p>criminal offences constitutes a change further development of the original purpose of Eurodac ; which interferes with the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac. In line with the requirements of Article 52(1) of the Charter of Fundamental Rights of the European Union, any such interference, 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.</p>		
<p>(21) Even though the original purpose of the establishment of</p>			

<p>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.</p>			
<p>(22) This Regulation also lays down the conditions under which requests for comparison of fingerprint data with Eurodac data for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences should be allowed and the necessary safeguards to ensure</p>	<p>Amendment 19</p> <p>(22) This Regulation also lays down the conditions under which requests for comparison of fingerprint biometric or alphanumeric data with Eurodac data for the purposes of preventing, detecting or</p>	<p>(22) 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</p>	

<p>the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac. The strictness of those conditions reflects the fact that the Eurodac database registers fingerprint data of persons who are not presumed to have committed a terrorist offence or other serious criminal offence.</p>	<p>investigating terrorist offences or other serious criminal offences should be allowed and the necessary safeguards to ensure the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in Eurodac. The strictness of those conditions reflects the fact that the Eurodac database registers fingerprint biometric and alphanumeric data of persons who are not presumed to have committed a terrorist offence or other serious criminal offence. <i>Law enforcement authorities and Europol do not always have the biometric data of the suspect, perpetrator or victim whose case they are investigating, which can hamper their ability to check biometric matching databases such as Eurodac. 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 such cases, in particular where those authorities and Europol possess evidence of the personal details or identity documents of the suspect, perpetrator or victim.</i></p>	<p>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 will not always have the biometric data of the perpetrator 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. Allowing for the possibility to search Eurodac based on alphanumeric data will contribute further to investigations carried out by law enforcement authorities and Europol, in particular in cases</p>	
--	---	--	--

		where no biometric evidence can be found, but where they may possess evidence of the personal data or identity documents of the perpetrator or of the victim.	
		(22a) The challenge of maintaining security in an open Europe has been put to a huge test in recent years. In view of the fact that threats are becoming more varied and more international, as well as increasingly cross-border and cross-sectorial in nature, the EU must do its utmost to help Member States protect citizens. Therefore, the expansion of the scope and simplification of law enforcement access to Eurodac should help Member States dealing with the increasingly complicated operational situations and cases involving cross-border crimes and terrorism with direct impact on the security situation in the EU. The conditions of access to Eurodac for the purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences should also allow the law enforcement authorities of	

		<p>the Member States to tackle the cases of suspects using multiple identities. For this purpose, obtaining a hit during a consultation of a relevant database prior to acceding Eurodac should not prevent such access. It may also be a useful tool to respond to the threat from radicalised persons or terrorists who may seek to re-enter the EU under the guise of an asylum-seeker. A broader and simpler access of law enforcement authorities of the Member States to Eurodac may, while guaranteeing the full respect of the fundamental rights, enable Member States to use all existing tools to ensure that people live in an area of freedom, security and justice.</p>	
<p>(23) With a view to ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with the current Union asylum acquis, in particular with Directive 2011/95/EU of the European Parliament and of the Council of</p>	<p>Amendment 20</p> <p>(23) With a view to ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with the current Union asylum acquis, in particular with Directive</p>	<p>(23) With a view to ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with the current Union asylum acquis, in particular with Directive 2011/95/EU of the European Parliament and of the Council²⁹ and Regulation (EU) No</p>	

<p>13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted²⁷ and Regulation (EU) No [.../...]604/2013, it is appropriate to extend the scope of this Regulation in order to include ☒ includes ☒ applicants for subsidiary protection and persons eligible for subsidiary protection ☒ in its scope ☒ .</p>	<p>2011/95/EU of the European Parliament and of the Council²⁸ and <i>with [Regulation XXX/XXX] establishing a Union Resettlement Framework</i> and Regulation (EU) No [.../...], this Regulation includes <i>in its scope</i> applicants for subsidiary protection and persons eligible for subsidiary protection in its scope, <i>as well as persons granted international protection on the basis of resettlement in accordance with [Regulation XXX/XXX]</i>.</p>	<p>XXX/XXX [Dublin Regulation] [...], this Regulation includes applicants for subsidiary protection and persons eligible for subsidiary protection in its scope.</p>	
<p>(24) It is also necessary to require the Member States promptly to take and transmit the fingerprint data of every applicant for international protection and of every third-country national or stateless person who is apprehended in connection with the irregular crossing of an</p>	<p>Amendment 21 (24) It is also necessary to require the Member States promptly to take and transmit the fingerprint biometric data of every applicant for international protection, of every <i>resettled third-country national or stateless</i></p>	<p>(24) It is also necessary to require the Member States promptly to take and transmit the biometric [...] data of every applicant for international protection and of every third-country national or stateless person who is apprehended in connection with the irregular crossing of an</p>	

²⁹ Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted (OJ L 337, 20.12.2011, p. 9).


²⁷ Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted (OJ L 337, 20.12.2011, p. 9).

²⁸ Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible

external border of a Member State ⇒ or is found to be staying illegally in a Member State ⇐, if they are at least 14 ⇒ six ⇐ years of age.	<i>person in accordance with [Regulation XXX/XXX]</i> and of every third-country national or stateless person who is apprehended in connection with the irregular crossing of an external border of a Member State or is found to be staying illegally in a Member State, if they are at least six years of age.	external border of a Member State or is found to be staying illegally in a Member State, if they are at least six years of age.	
			Confirmed by trilogue (link to EP amendment 92) <i>(24a) 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.</i>
(25) In view of strengthening the protection of unaccompanied minors who have not applied for international protection and those children who may become separated from their families, it is also necessary to take fingerprints and a facial image for storage in	Amendment 22 (25) In view of strengthening the protection of <i>all migrant and refugee children, including</i> unaccompanied minors who have not applied for international protection and those children who may become separated from their	(25) In view of strengthening the protection of unaccompanied minors who have not applied for international protection and those children who may become separated from their families, it is also necessary to take biometric data [...] for storage in the Central	Confirmed by trilogue (link to EP amendment in Art. 2a(5)) (25) In view of strengthening the protection of <i>all children falling under the scope of this Regulation, including</i> unaccompanied minors who have not applied for international protection and those

<p>the Central System to help establish the identity of a child and assist a Member State to trace any family or links they may have with another Member State. Establishing family links is a key element in restoring family unity and must be is closely linked to the determination of the best interests of the child and eventually, the determination of a durable solution.</p>	<p>families, it is also necessary to take fingerprints and a facial image biometric data for storage in the Central System to help establish the identity of a child and assist a Member State to trace any family or links they may have with another Member State. <i>Biometric data should be taken for that sole purpose, and should be processed and used accordingly.</i> Establishing family links is a key element in restoring family unity and must be closely linked to the determination of the best interests of the child and eventually, the determination of a durable sustainable solution. <i>In the performance of those tasks, Member States should observe the principles laid down in the United Nations Convention on the Rights of the Child of 1989. Improved identification procedures for missing children should assist Member States in guaranteeing that adequate protection of children is ensured. To that end, Member States, upon the identification of a missing child or of a child who is the victim of crime, should promptly contact the competent national child protection authorities, which</i></p>	<p>System to help establish the identity of a child and assist a Member State to trace any family or links they may have with another Member State. Establishing family links is a key element in restoring family unity and must be closely linked to the determination of the best interests of the child and eventually, the determination of a durable solution.</p>	<p>children who may become separated from their families, it is also necessary to take biometric data for storage in the Central System to help establish the identity of children and assist a Member State in tracing any family or links they may have with another Member State, <i>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.</i> 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 <i>in accordance with national practices following a needs assessment by the competent national child protection authorities.</i></p>
---	---	--	--

	<i>should undertake a needs assessment with a view to finding a sustainable solution for the child in accordance with his or her best interests.</i>		
		(25a) All minors from the age of six years old and above, including unaccompanied minors, should be accompanied at the time their biometric data is being captured for the purposes of Eurodac by a [legal representative, guardian] or a person trained to safeguard the best interest of the child and his or her general well-being. The official responsible for taking the biometric data of a minor should also receive training so that sufficient care is taken to ensure an adequate quality of fingerprints of the minor and to guarantee that the process is child-friendly so that the minor, particularly a very young minor, feels safe and can readily cooperate with the process for having his or her biometric data taken.	
(26) The best interests of the minor should be a primary consideration for Member States	Amendment 23 (26) The best interests of the		

<p>when applying this Regulation. Where the requesting Member State establishes that Eurodac data pertain to a child, these data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws applicable to minors and in accordance with the obligation to give primary consideration to the best interests of the child.</p>	<p>minor should be a primary consideration for Member States when applying this Regulation. Where the requesting Member State establishes that Eurodac data pertain to a child, these <i>those</i> data may only be used for law enforcement purposes, <i>in particular those relating to the prevention, detection and investigation of child trafficking and other serious crimes against children</i>, by the requesting Member State <i>and</i> 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.</p>		
<p>(27) It is necessary to lay down precise rules for the transmission of such fingerprint ⇨ and facial image ⇐ data to the Central System, the recording of such fingerprint ⇨ and facial image ⇐ data and of other relevant ☒ personal ☒ data in the Central System, their storage, their comparison with other fingerprint ⇨ and facial image ⇐ data, the transmission of the results of such comparison and the marking and erasure of the recorded data. Such</p>		<p>(27) It is necessary to lay down precise rules for the transmission of such biometric [...] data to the Central System, the recording of such biometric [...] data and of other relevant personal data in the Central System, their storage, their comparison with other biometric [...] data, the transmission of the results of such comparison and the marking and erasure of the recorded data. Such rules may be different for, and should be specifically adapted to, the</p>	

rules may be different for, and should be specifically adapted to, the situation of different categories of third-country nationals or stateless persons.		situation of different categories of third-country nationals or stateless persons.	
---	--	--	--

<p>(28) Member States should ensure the transmission of fingerprint ⇨ and facial image ⇦ data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint ⇨ and facial ⇦ recognition system. All authorities with a right of access to Eurodac should invest in adequate training and in the necessary technological equipment. The authorities with a right of access to Eurodac should inform the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council³⁰ (the "Agency" ⇨ "eu-LISA" ⇦) of specific difficulties encountered with regard to the quality of data, in order to resolve them.</p>		<p>(28) Member States should ensure the transmission of biometric [...] data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint and facial recognition system. All authorities with a right of access to Eurodac should invest in adequate training and in the necessary technological equipment. The authorities with a right of access to Eurodac should inform [...] ³¹ eu-LISA [...] of specific difficulties encountered with regard to the quality of data, in order to resolve them.</p>	
<p>(29) The fact that it is temporarily or permanently impossible to take and/or to transmit fingerprint ⇨ and facial image ⇦ data, due to reasons such</p>		<p>(29) The fact that it is temporarily or permanently impossible to take and/or to transmit biometric [...] data, due to reasons such as insufficient</p>	

³⁰ Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p. 1).

³¹ [...]

as insufficient quality of the data for appropriate comparison, technical problems, reasons linked to the protection of health or due to the data subject being unfit or unable to have his or her fingerprints ⇨ or facial image ⇦ taken owing to circumstances beyond his or her control, should not adversely affect the examination of or the decision on the application for international protection lodged by that person.		quality of the data for appropriate comparison, technical problems, reasons linked to the protection of health or due to the data subject being unfit or unable to have his or her biometric data [...] taken owing to circumstances beyond his or her control, should not adversely affect the examination of or the decision on the application for international protection lodged by that person.	
(30) Member States should refer to the Commission's Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints adopted by the Council on 20 July 2015 ³² , which sets out a best practice approach to taking fingerprints of irregular third-country nationals. Where a Member State's national law allows for the taking of fingerprints by force or coercion as a last resort, those measures must fully respect the EU Charter	Amendment 24 (30) <i>In order to ensure that all the persons referred to in Article 10(1), 12a, 13(1) and 14(1) are registered in Eurodac,</i> Member States should refer to the Commission's Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints adopted by the Council on 20 July 2015 ³³ , which sets out a best practice approach to taking fingerprints of irregular third-country nationals <i>or stateless</i>	(30) Member States should refer to the Commission's Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints which [...] the Council invited the Member States to follow on 20 July 2015 ³⁴ , which sets out a best practice approach to taking fingerprints of irregular third-country nationals or stateless persons . Where a Member State's national law allows for the taking of fingerprints by force or coercion as a last resort, those measures must fully respect the EU Charter	<i>Informal outcome of technical discussions, pending agreement on the last sentence linked to Art. 2(3) and 2a(1)</i> (30) 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 ³⁵ . <i>It sets out a best practice approach to taking fingerprints of irregular migrants or asylum seekers. Where relevant, Member States should also</i>

³² COM(2015) 150 final, 27.5.2015

³³ **COM(2015) 0150.**

³⁴ SWD(2015) 150 final, 27.5.2015

³⁵ SWD(2015) 150 final, 27.5.2015

<p>of Fundamental Rights. Third-country nationals who are deemed to be vulnerable persons and minors should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law.</p>	<p><i>persons. When carrying out that process, Member States should also take account of the guidelines established by the European Union Agency for Fundamental Rights in its focus paper of May 2015 entitled "Fundamental rights implications of the obligation to provide fingerprints for Eurodac". Where a Member State's national law allows for the taking of fingerprints by force or coercion as a last resort, those measures must fully respect the Charter of Fundamental Rights</i> Third-country nationals who are deemed to be vulnerable persons and minors should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law of the European Union. Where a minor, in particular an unaccompanied or separated minor, refuses to give his or her fingerprints or facial image and there are reasonable grounds for believing that there are child safeguarding or protection risks, that minor should be referred to</p>	<p>of Fundamental Rights. Third-country nationals or stateless persons who are deemed to be vulnerable persons and minors should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law. In this context, detention should only be used as a means of last resort in order to determine or verify a third-country national's or stateless person's identity.</p>	<p>take into account, where relevant, the Checklist to act in compliance with fundamental rights when obtaining fingerprints for Eurodac of the European Union Agency for Fundamental Rights³⁶ which aims to assist them with complying with fundamental rights obligations when taking fingerprints, in particular with regard to the content and form of the information to be provided, the use of measures alternative to coercion, the need to avoid the use of force, and the treatment of children and vulnerable persons. 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 coercion as a last resort, those measures must fully respect the Charter of Fundamental Rights of the European Union. [Third-country nationals or stateless persons who are deemed to be vulnerable persons, including</p>
--	---	---	--

³⁶ 'Fundamental rights implications of the obligation to provide fingerprints for Eurodac', FRA Focus paper, 5/2015

	<i>the competent national child protection authorities, national referral mechanisms, or both. Those authorities should undertake an assessment of the minor's special needs in accordance with the relevant law with a view to finding a sustainable solution for the minor in full respect of the best interests of the child.</i>		minors, should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law.]
			Confirmed by trilogue <i>(30a) 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 Charter of Fundamental Rights of the European Union.</i>
(31) Hits obtained from Eurodac should be verified by a trained fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No 604/2013 ⇒; the exact identification of the third-country	Amendment 25 (31) Hits obtained from Eurodac should be verified by a trained fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [.../...], the exact identification of	(31) Hits obtained from Eurodac should be verified by a trained fingerprint expert, where necessary , in order to ensure the accurate determination of responsibility under Regulation (EU) No XXX/XXX [Dublin Regulation] [...]; the exact	Informal outcome of technical discussion (link to Article 26(4) and (5)) (31) <u>Where necessary, hits obtained from Eurodac</u> should be <u>checked</u> verified by a trained fingerprint expert where necessary , in order to ensure the accurate

<p>national or stateless person ⇐ and the exact identification of the criminal suspect or victim of crime whose data might be stored in Eurodac. ⇒ Hits obtained from Eurodac based on facial images should also be verified where there is doubt that the result relates to the same person. ⇐</p>	<p>the third-country national or stateless person and the exact identification of the criminal suspect or victim of crime whose data might be stored in Eurodac. Hits obtained from Eurodac based on facial images should also be verified where there is doubt that the result relates to the same person <i>by an official trained in accordance with national practice, in particular where the comparison is made with a facial image only. Where a fingerprint and facial image comparison is carried out simultaneously and a hit is received for both biometric data sets, Member States may check and verify the facial image result, if needed.</i></p>	<p>identification of the third-country national or stateless person and the exact identification of the criminal suspect or victim of crime whose data might be stored in Eurodac. Hits obtained from Eurodac based on facial images should also be verified by an official trained in accordance with national practice, particularly where the comparison is made with a facial image only. Where a fingerprint and facial image comparison is carried out simultaneously and a hit result is received for both biometric data sets, Member States may check and verify the facial image result, if needed [...].</p>	<p>determination of responsibility under Regulation (EU) No XXX/XXX [Dublin Regulation] [...], 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.</p> <p><u><i>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.</i></u></p> <p>Hits obtained from Eurodac based on facial images should also be <u>checked</u> verified by an official trained in accordance with national practice, particularly where the comparison is made with a facial image <u>data</u> only.</p> <p>Where a fingerprint and facial image <u>data</u> comparison is carried out simultaneously and <u>two hits are returned</u> received for both</p>
---	---	--	---

			biometric data sets, Member States should be able to may check and verify the result of the comparison of the facial image data.
<p>(32) Third-country nationals or stateless persons who have requested international protection in one Member State may have the option of ⇨ try to ⇐ requesting international protection in another Member State for many years to come. Therefore, the maximum period during which fingerprint ⇨ and facial image ⇐ data should be kept by the Central System should be of considerable length. Given that most third-country nationals or stateless persons who have stayed in the Union for several years will have obtained a settled status or even citizenship of a Member State after that period, a period of ten years should be considered a reasonable period for the storage of fingerprint ⇨ and facial image ⇐ data.</p>	<p>Amendment 26</p> <p>(32) <i>The maximum period during which biometric data of</i> third-country nationals or stateless persons who have requested international protection in one Member State may try to request international protection in another Member State for many years to come. Therefore, the maximum period during which fingerprint and facial image data should be kept by the Central System should be of considerable length <i>can be kept by the Central System 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 the Court of Justice.</i> 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</p>	<p>(32) Third-country nationals or stateless persons who have requested international protection in one Member State may try to request international protection in another Member State for many years to come. Therefore, the maximum period during which biometric [...] data should be kept by the Central System should be of considerable length. Given that most third-country nationals or stateless persons who have stayed in the Union for several years will have obtained a settled status or even citizenship of a Member State after that period, a period of ten years should be considered a reasonable period for the storage of biometric [...] data.</p>	

	<p>ten five years should be considered a reasonable period for the storage of fingerprint and facial image biometric data.</p>		
	<p>Amendment 27</p> <p><i>(32 a) 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. In its resolution of 25 October 2016 on human rights and migration in third countries, the European Parliament recalled the importance of identifying stateless persons in order to afford them the protections available under international law.</i></p>		
<p>(33) In view of successfully preventing and monitoring unauthorised movements of third-country nationals or stateless persons who have no right to stay</p>	<p>Amendment 28</p> <p>(33) In view of successfully preventing and monitoring unauthorised movements of third-country nationals or stateless</p>	<p>(33) In view of successfully preventing and monitoring unauthorised movements of third-country nationals or stateless persons who have no right to stay</p>	

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 ³⁷ and the right to protection of personal data, a period of five years should be considered a necessary period for the storage of fingerprint and facial data.	persons who have no right to stay in the Union, and of taking the necessary measures for successfully enforcing effective return and readmission to third countries in accordance with Directive 2008/115/EC ³⁸ and the right to protection of personal data, a period of five years should be considered a necessary period for the storage of fingerprint and facial biometric and alphanumeric data.	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 ³⁹ and the right to protection of personal data, a period of five years should be considered a necessary period for the storage of biometric [...] data.	
(34) The storage period should be shorter in certain special situations where there is no need to keep fingerprint ⇨ and facial ⇩ data ⇨ and all other personal data ⇩ for that length of time. Fingerprint ⇨ and facial image ⇩ data ⇨ and all other personal data belonging to a third-country national ⇩ should be erased immediately once third-country nationals or stateless persons obtain citizenship of a Member State.	Amendment 29 (34) The storage period should be shorter in certain special situations where there is no need to keep fingerprint and facial biometric data and all other personal data for that length of time. Fingerprint and facial image 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	(34) The storage period should be shorter in certain special situations where there is no need to keep biometric [...] data and all other personal data for that length of time. Biometric [...] data and all other personal data belonging to a third-country national or a stateless person should be erased immediately once third-country nationals or stateless persons obtain citizenship of a Member State.	

³⁷ OJ L 348, 24.12.2008, p.98

³⁸ OJ L 348, 24.12.2008, p.98

³⁹ OJ L 348, 24.12.2008, p.98


	of a Member State.		
<p>(35) It is appropriate to store data relating to those data subjects whose fingerprints ⇨ and facial images ⇨ were initially recorded in Eurodac upon lodging their applications for international protection and who have been granted international protection in a Member State in order to allow data recorded upon lodging an application for international protection to be compared against them.</p>		<p>(35) It is appropriate to store data relating to those data subjects whose biometric data [...] were initially recorded in Eurodac upon lodging their applications for international protection and who have been granted international protection in a Member State in order to allow data recorded upon lodging an application for international protection to be compared against them.</p>	
<p>(36) The Agency ⇨ eu-LISA ⇨ has been entrusted with the Commission's tasks relating to the operational management of Eurodac in accordance with this Regulation and with certain tasks relating to the Communication Infrastructure as from the date on which the Agency ⇨ eu-LISA ⇨ took up its responsibilities on 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation, and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should have observer status at the meetings of the</p>			


<p>Management Board of the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> 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 <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> the Agency.</p>			
<p>The Staff Regulations of Officials of the European Union (Staff Regulations of Officials) and the Conditions of Employment of Other Servants of the European Union ('Conditions of Employment'), laid down in Regulation (EEC, Euratom, ECSC) No 259/68 of the Council⁴⁰ (together referred to as the 'Staff Regulations') should apply to all staff working in the Agency on matters pertaining to this Regulation.</p>			
<p>(37) It is necessary to lay down</p>	<p>Amendment 30</p>	<p>(37) It is necessary to lay down</p>	

⁴⁰ ~~OJ L 56, 4.3.1968, p. 1.~~

clearly the respective responsibilities of the Commission and eu-LISA the Agency , in respect of the Central System and the Communication Infrastructure, and of the Member States, as regards data processing, data security, access to, and correction of ² recorded data.	(37) It is necessary to lay down clearly the respective responsibilities of the Commission and eu-LISA, in respect of the Central System and the Communication Infrastructure and interoperability with other information systems , and of the Member States, as regards data processing, data security, access to, and correction of recorded data.	clearly the respective responsibilities of the Commission and eu-LISA, in respect of the Central System and the Communication Infrastructure, and of the Member States, as regards data processing, data security, access to, and rectification [...] of recorded data.	
(38) It is necessary to designate the competent authorities of the Member States as well as the National Access Point through which the requests for comparison with Eurodac data are made and to keep a list of the operating units within the designated authorities that are authorised to request such comparison for the specific purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.			
			Confirmed by trilogue (link to EP amendment 69 in Art. 8(2a)) (38a) It is necessary to designate and keep a list of the operating unit(s) of Europol that are authorised to request comparisons with Eurodac

			<i>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.</i>
<p>(39) Requests for comparison with data stored in the Central System should be made by the operating units within the designated authorities to the National Access Point, through the verifying authority, and should be reasoned. The operating units within the designated authorities that are authorised to request comparisons with Eurodac data should not act as a verifying authority. The verifying authorities should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for</p>			

<p>access as established in this Regulation. The verifying authorities should then forward the request, without forwarding the reasons for it, for comparison through the National Access Point to the Central System following verification that all conditions for access are fulfilled. In exceptional cases of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the verifying authority should process the request immediately and only carry out the verification afterwards.</p>			
<p>(40) The designated authority and the verifying authority may be part of the same organisation, if permitted under national law, but the verifying authority should act independently when performing its tasks under this Regulation.</p>			
<p>(41) For the purposes of protection of personal data, and to exclude systematic comparisons which should be forbidden, the processing of Eurodac data should only take place in specific cases and when it is necessary for the</p>			

<p>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.</p>			
<p>(42) In addition, access should be allowed only on condition that comparisons with the national fingerprint databases of the</p>	<p>Amendment 31</p> <p>(42) In addition, access should be allowed only on condition that</p>	<p>(42) In addition, access should be allowed only on condition that a prior search in [...] the national biometric [...] databases of the</p>	

<p>Member State and with the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime⁴¹ did not lead to the establishment of the identity of the data subject. That condition requires the requesting Member State to conduct comparisons with the automated fingerprinting identification systems of all other Member States under Decision 2008/615/JHA which are technically available, unless that Member State can justify that there are reasonable grounds to believe that it would not lead to the establishment of the identity of the data subject. Such reasonable grounds exist in particular where the specific case does not present any operational or investigative link to a given Member State. That</p>	<p>comparisons with a prior search in the national fingerprint and facial image databases of the Member State and with in the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA⁴² did not lead to the establishment of the identity of the data subject has been conducted. That condition requires the requesting Member State to conduct comparisons with the automated fingerprinting identification systems of all other Member States under Decision 2008/615/JHA which are technically available, unless that Member State can justify that there are reasonable grounds to believe that it would not lead to the establishment of the identity of the data subject. Such reasonable grounds exist in particular where the specific case does not present any operational or investigative link to a given Member State. That condition requires prior legal and</p>	<p>Member State and in [...] the automated fingerprinting identification systems of all other Member States under Council Decision 2008/615/JHA⁴³ has been conducted [...]. That condition requires the requesting Member State to conduct comparisons with the automated fingerprinting identification systems of all other Member States under Decision 2008/615/JHA which are technically available, unless that Member State can justify that there are reasonable grounds to believe that it would not lead to the establishment of the identity of the data subject. Such reasonable grounds exist in particular where the specific case does not present any operational or investigative link to a given Member State. That condition requires prior legal and technical implementation of Decision 2008/615/JHA by the requesting Member State in the area of fingerprint data, as it should not be</p>	
---	--	---	--

⁴¹ 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).

⁴² 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).

⁴³ 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).

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.	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.	permitted to conduct a Eurodac check for law enforcement purposes where those above steps have not been first taken.	
(43) Prior to searching Eurodac, designated authorities should also, provided that the conditions for a comparison are met, consult the Visa Information System under Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences ⁴⁴ .	Amendment 32 (43) Prior to searching Eurodac, designated authorities should also, provided that the conditions for a comparison are met, consult the Visa Information System under Council Decision 2008/633/JHA ⁴⁵ . <i>deleted</i>	(43) [...]	
(44) For the purpose of efficient comparison and exchange of			

⁴⁴ Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

⁴⁵ ~~Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).~~

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.			
The best interests of the child should be a primary consideration for Member States when applying this Regulation. Where the requesting Member State establishes that Eurodac data pertain to a minor, these data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws applicable to minors and in accordance with the obligation to give primary consideration to the best interests of the child.			
(45) While the non-contractual liability of the Union in connection with the operation of the Eurodac system will be governed by the relevant provisions of the Treaty on the Functioning of the European Union (TFEU), it is necessary to lay down specific rules for the			

non-contractual liability of the Member States in connection with the operation of the system.			
(46) Since the objective of this Regulation, namely the creation of a system for the comparison of fingerprint ⇨ and facial image ⇐ data to assist the implementation of Union asylum ☒ and migration ☒ policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.		(46) Since the objective of this Regulation, namely the creation of a system for the comparison of biometric [...] data to assist the implementation of Union asylum and migration policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	
(47) [Directive [2016/.../...] of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ⁴⁶] applies		(47) Directive (EU)2016/680 [...]of the European Parliament and of the Council ⁴⁷ applies to the processing of personal data by the Member States carried out in application of this Regulation unless such processing is carried	

⁴⁶

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

<p>to the processing of personal data by the Member States carried out in application of this Regulation unless such processing is carried out by the designated or verifying competent authorities of the Member States for the purposes of the prevention, investigation, detection or investigation prosecution of terrorist offences or of other serious criminal offences including the safeguarding against and the prevention of threats to public security .</p>		<p>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.</p>	
<p>(48) competent The national provisions adopted pursuant to Directive [2016/... /EU] of the European Parliament and of the Council [of ... 2016] on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data apply to the the processing of personal data by the</p>		<p>(48) 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</p>	

<p> <input checked="" type="checkbox"/> competent <input checked="" type="checkbox"/> authorities of the Member States for the purposes of the prevention, <input checked="" type="checkbox"/> investigation, <input checked="" type="checkbox"/> detection or investigation <input checked="" type="checkbox"/> prosecution <input checked="" type="checkbox"/> of terrorist offences or of other serious criminal offences pursuant to this Regulation should be subject to a standard of protection of personal data under their national law which complies with Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters⁴⁸. </p>		<p> 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. </p>	
<p> (49) The principles <input checked="" type="checkbox"/> rules <input checked="" type="checkbox"/> set out in Regulation Directive [2016/.../...] 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to <input checked="" type="checkbox"/> the protection of personal data concerning them <input checked="" type="checkbox"/> privacy, with regard to the processing of personal data should be <input checked="" type="checkbox"/> 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 <input checked="" type="checkbox"/> </p>		<p> (49) The rules set out in Regulation 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 </p>	

⁴⁸ ~~OJ L 350, 30.12.2008, p. 60.~~

supplemented or clarified, in particular as far as certain sectors are concerned.		as certain sectors are concerned.	
			<p><i>Under discussion - EP proposal (link to EP amendment 137 in Art. 31(2))</i></p> <p><i>(49a) 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 2016/679 and in accordance with the procedures set out in this Regulation, Directive 2016/680 and Regulation 2016/794 as regards the processing of personal data for law enforcement purposes pursuant to this Regulation.</i></p>
(50) Transfers of personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System to any third country or	<p>Amendment 33</p> <p>(50) Transfers of personal data obtained by a Member State or Europol pursuant to this</p>	(50) Transfers of personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System to any third country or	

<p>international organisation or private entity established in or outside the Union should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to a third country. This implies that Member States should not transfer information obtained from the Central System concerning: ⇒ the name(s); date of birth; nationality; ⇐ the Member State(s) of origin ⇒ or Member State of allocation; the details of the identity or travel document; ⇐ ; the place and date of application for international protection; the reference number used by the Member State of origin; the date on which the fingerprints were taken as well as the date on which the Member State(s) transmitted the data to Eurodac; the operator user ID; and any information relating to any transfer of the data subject under [Regulation (EU) No 604/2013]. That prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which [Regulation (EU) No 604/2013] applies [⇒ in accordance with Regulation (EU)</p>	<p>Regulation from the Central System to any third country or international organisation or private entity established in or outside the Union should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection and resettled third-country nationals and stateless persons in accordance with [Regulation XXX/XXX] from having their data disclosed to a third country. This implies that Member States should not transfer information obtained from the Central System concerning: the name(s); date of birth; nationality; the Member State(s) of origin or Member State of allocation 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 fingerprints were taken as well as the date on which the Member State(s) transmitted the data to Eurodac; the operator user ID; and any information relating to any transfer of the data subject under [Regulation (EU) No</p>	<p>international organisation or private entity established in or outside the Union should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to a third country. This implies that Member States should not transfer information obtained from the Central System concerning: the name(s); date of birth; nationality; the Member State(s) of origin [or Member State of allocation;] the details of the identity or travel document; the place and date of application for international protection; the reference number used by the Member State of origin; the date on which the biometric data[...]were taken as well as the date on which the Member State(s) transmitted the data to Eurodac; the operator user ID; and any information relating to any transfer of the data subject under Regulation (EU) No XXX/XXX [Dublin Regulation] [...]. That prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No XXX/XXX [Dublin</p>
---	--	--

<p>No [.../2016]respectively with the national rules adopted pursuant to Directive [2016/.../EU] ⇄], in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.</p>	<p>604/2013]. That prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which [Regulation (EU) No 604/2013] applies [in accordance with Regulation (EU) No [.../2016] respectively with the national rules adopted pursuant to Directive [2016/.../EU]], in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.</p>	<p>Regulation] [...] applies in accordance with Regulation (EU) No 2016/679 and [...] with the national rules adopted pursuant to Directive 2016/680/EU [...], in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.</p>	
<p>(51) In individual cases, information obtained from the Central System may be shared with a third-country in order to assist with the identification of a third-country national in relation to his/her return. Sharing of any personal data must be subject to strict conditions. Where such information is shared, no information shall be disclosed to a third-country relating to the fact that an application for international protection has been made by a third-country national where the country the individual is being readmitted to, is also the individual's country of origin or another third-country where they</p>	<p>Amendment 34</p> <p>(51) In individual cases, information obtained from the Central System may be shared with a third-country in order to assist with the identification of a third-country national or a stateless person in relation to his/her return. Sharing of any personal data must be subject to strict conditions. Where such information is shared, no information shall be disclosed to a third-country relating to the fact that an application for international protection has been made by a third-country national or a stateless person where the</p>	<p>(51) In individual cases, information obtained from the Central System may be shared with a third-country in order to assist with the identification of a third-country national or a stateless person in relation to his/her return. Sharing of any personal data must be subject to strict conditions. Where such information is shared, no information shall be disclosed to a third-country relating to the fact that an application for international protection has been made by a third-country national or a stateless person where the country the individual is being readmitted to, is also the individual's country</p>	

will be readmitted. Any transfer of data to a third-country for the identification of a third-country national must be in accordance with the provisions of Chapter V of Regulation (EU) No. [...2016].	country the individual is being readmitted to, is also the individual's country of origin or another third-country where they will be readmitted. Any transfer of data to a third-country for the identification of a third-country national <i>or a stateless person</i> must be in accordance with the provisions of Chapter V of Regulation (EU) No. [679/2016].	of origin or another third-country where they will be readmitted. Any transfer of data to a third-country for the identification of a third-country national or stateless person must be in accordance with the provisions of Chapter V of Regulation (EU) No. 679/2016 [...].	
(52) National supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by Decision 2009/371/JHA should monitor the lawfulness of data processing activities performed by Europol.		(52) National supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States, and the European Data Protection Supervisor [...] should monitor the lawfulness of data processing activities performed by Europol in accordance with Regulation (EU) 2016/794 .	
(53) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community		(53) Regulation (EC) No 45/2001 of the European Parliament and of the Council ⁵⁰ , and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing, applies to the processing of personal data	

<p>institutions and bodies and on the free movement of such data⁴⁹, and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing, applies to the processing of personal data by Union institutions, bodies, offices and agencies carried out in application of this Regulation. However, certain points should be clarified in respect of the responsibility for the processing of data and of the supervision of data protection, bearing in mind that data protection is a key factor in the successful operation of Eurodac and that data security, high technical quality and lawfulness of consultations are essential to ensure the smooth and proper functioning of Eurodac as well as to facilitate the application of [Regulation (EU) No 604/2013].</p>		<p>by Union institutions, bodies, offices and agencies carried out in application of this Regulation. However, certain points should be clarified in respect of the responsibility for the processing of data and of the supervision of data protection, bearing in mind that data protection is a key factor in the successful operation of Eurodac and that data security, high technical quality and lawfulness of consultations are essential to ensure the smooth and proper functioning of Eurodac as well as to facilitate the application of Regulation (EU) No XXX/XXX [Dublin Regulation] [...].</p>	
<p>(54) The data subject should be informed ⇨ in particular ⇨ of the purpose for which his or her data will be processed within Eurodac, including a description of the aims</p>		<p>(54) The data subject should be informed in particular of the purpose for which his or her data will be processed within Eurodac, including a description of the aims</p>	


⁵⁰ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

⁴⁹ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

of Regulation (EU) [...] No 604/2013 , and of the use to which law enforcement authorities may put his or her data.		of Regulation (EU) XXX/XXX [Dublin Regulation] [...], and of the use to which law enforcement authorities may put his or her data.	
(55) It is appropriate that national supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor, as referred to in Regulation (EC) No 45/2001, should monitor the activities of the Union institutions, bodies, offices and agencies in relation to the processing of personal data carried out in application of this Regulation.			
(56) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on [...]		(56) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 21 September 2016 .	
(57) Member States, the European Parliament, the Council and the Commission should ensure that the national and European supervisory authorities are able to supervise the use of and access to Eurodac data adequately.			

<p>(58) It is appropriate to monitor and evaluate the performance of Eurodac at regular intervals, including in terms of whether law enforcement access has led to indirect discrimination against applicants for international protection, as raised in the Commission's evaluation of the compliance of this Regulation with the Charter of Fundamental Rights of the European Union ('the Charter'). The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> should submit an annual report on the activities of the Central System to the European Parliament and to the Council.</p>		<p>(58) It is appropriate to monitor and evaluate the performance of Eurodac at regular intervals [...]. eu-LISA should submit an annual report on the activities of the Central System to the European Parliament and to the Council.</p>	
<p>(59) Member States should provide for a system of effective, proportionate and dissuasive penalties to sanction the <input checked="" type="checkbox"/> unlawful <input checked="" type="checkbox"/> processing of data entered in the Central System contrary to the purpose of Eurodac.</p>			
<p>(60) It is necessary that Member States be informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No 604/2013.</p>		<p>(60) It is necessary that Member States be informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No XXX/XXX [Dublin Regulation]</p>	

		[...].	
(61) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter. In particular, this Regulation seeks to ensure full respect for the protection of personal data and for the right to seek international protection, and to promote the application of Articles 8 and 18 of the Charter. This Regulation should therefore be applied accordingly.			
(62) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.			
In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the TEU and to the TFEU, the United Kingdom has notified its wish to take part in the adoption and application of this Regulation.			

<p>In accordance with Article 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the TEU and to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.</p>			
<p>(63) [In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, those Member States have notified their wish to take part in the adoption and application of this Regulation] OR</p>		<p>(63) [...]</p>	
<p>(64) [In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without</p>		<p>(64) [...]</p>	

prejudice to Article 4 of that Protocol, those Member States are not taking part in the adoption of this Regulation and are not bound by it or subject to its application.] OR			
(65) [In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, the United Kingdom is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.]		(65) [...]	
(66) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Ireland has notified (, by letter of ...,) its wish to take part in the adoption and application of this Regulation.] OR		(66) [...]	

<p>(67) [In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom has notified (, by letter of ...,) its wish to take part in the adoption and application of this Regulation.</p>		<p>(67) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom has notified, by letter of 17 November 2016, its wish to take part in the adoption and application of this Regulation.</p>	
<p>(68) In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.]</p>			
<p>(69) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of Regulation (EU) No [.../...] 604/2013,</p>		<p>(69) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of Regulation (EU) No XXX/XXX [Dublin Regulation] [...],</p>	

HAVE ADOPTED THIS REGULATION:		HAVE ADOPTED THIS REGULATION:	
CHAPTER I		CHAPTER I	
<i>GENERAL PROVISIONS</i>		<i>GENERAL PROVISIONS</i>	
<i>Article 1</i>		<i>Article 1</i>	
Purpose of "Eurodac"		Purpose of "Eurodac"	
1. A system known as "Eurodac" is hereby established, the purpose of which shall be to:			
(a) assist in determining which Member State is to be responsible pursuant to Regulation (EU) No [...] 604/2013 for examining an application for international protection lodged in a Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No [...] 604/2013 under the conditions set out in this Regulation;		(a) assist in determining which Member State is to be responsible pursuant to Regulation (EU) No XXX/XXX [Dublin Regulation] [...] for examining an application for international protection lodged in a Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No XXX/XXX [Dublin Regulation] [...] under the conditions set out in this Regulation;	(a) assist in determining which Member State is to be responsible pursuant to Regulation (EU) No XXX/XXX [Dublin Regulation] [...] for examining an application for international protection lodged in a Member State by a third-country national or a stateless person, and otherwise to facilitate the application of Regulation (EU) No XXX/XXX [Dublin Regulation] under the conditions set out in this Regulation;
	Amendment 35		<i>The Council does not have a mandate</i>

	<i>(aa) assist with the identification of secondary movements of third-country nationals or stateless persons resettled in accordance with [Regulation XXX/XXX];</i>		<i>yet to discuss this text with the EP.</i>
(b) assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation.	Amendment 36 (b) assist with the control of illegal immigration to and secondary movements within the Union and with the identification of secondary movements and of illegally staying third-country nationals and stateless persons for determining the appropriate measures to be taken by Member States, including removal and repatriation of persons residing without authorisation as appropriate, removal and return of illegally staying third-country nationals and stateless persons, or granting permanent resident status;	(b) assist with the control of illegal immigration to and secondary movements within the Union and with the identification of illegally staying third-country nationals and stateless persons for determining the appropriate measures to be taken by Member States, including removal and returns of persons staying illegally [...].	<i>Confirmed by trilogue</i> (b) assist with the control of illegal 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. including, [as appropriate,] returns of illegally staying third-country nationals and stateless persons, [or granting permanent resident status;]
2. (c) This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint ⇨ and facial image ⇐	Amendment 37 (c) lay down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of	(c) lay down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of biometric or alphanumeric [...] data with those stored in the	<i>Confirmed by trilogue</i> (c) lay down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of biometric or

data with those stored in the Central System for law enforcement purposes ⇒ for the prevention, detection or investigation of terrorist offences or of other serious criminal offences ⇐ .	fingerprint and facial image biometric data and alphanumeric data with those stored in the Central System for law enforcement purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. <i>This Regulation shall also lay down the conditions under which the European Police Office (Europol) may request comparisons with Eurodac data for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences falling within its mandate.</i>	Central System for law enforcement purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.	alphanumeric [...] data with those stored in the Central System for law enforcement purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. <i>{This Regulation shall also lay down the conditions under which the European Police Office (Europol) may request comparisons with Eurodac data for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences falling within its mandate.}</i>
32. Without prejudice to the processing of data intended for Eurodac by the Member State of origin in databases set up under the latter's national law, fingerprint data and other personal data may be processed in Eurodac only for the purposes set out in this Regulation and [Article 34(1) of Regulation (EU) No 604/2013].	Amendment 38 2. Without prejudice to the processing of data intended for Eurodac by the Member State of origin in databases set up under the latter's national law, fingerprint , fingerprints and facial image data and other personal data may be processed in Eurodac only for the purposes set out in this Regulation and [Article 34(1) of Regulation (EU) No 604/2013]. <i>The data of minors may be used by the Member States for the</i>	2. Without prejudice to the processing of data intended for Eurodac by the Member State of origin in databases set up under the latter's national law, biometric [...] data and other personal data may be processed in Eurodac only for the purposes set out in this Regulation and Article [32, 33 and 48(1)(b)] [...] of Regulation (EU) No XXX/XXX [Dublin Regulation] [...].	<i>Confirmed by trilogue</i> 2. Without prejudice to the processing of data intended for Eurodac by the Member State of origin in databases set up under the latter's national law, biometric data and other personal data may be processed in Eurodac only for the purposes set out in this Regulation and in [Regulation (EU) No XXX/XXX (Dublin Regulation)].

	<i>purposes of assisting them in the identification and tracing of missing children and of establishing family links of unaccompanied minors.</i>		
Article 2		Article 2	
Obligation to take fingerprints and a facial image		Obligation to take <u>biometric data</u> [...]	Obligation to take <u>biometric data</u>
1. Member States are obliged to take the fingerprints and facial image of persons referred to in Article 10(1), 13(1) and 14(1) for the purposes of Article 1(1)(a) and (b) of this Regulation and shall impose on the data-subject the requirement to provide his or her fingerprints and a facial image and inform them as such in accordance with Article 30 of this Regulation.	Amendment 39 1. Member States are obliged to take the fingerprints and facial image of persons referred to in Article 10(1), 13(1) and 14(1) <i>The persons referred to in Articles 10(1), 13(1) and 14(1) shall be registered. Therefore, Member States shall take those person's biometric data</i> for the purposes of Article 1(1)(a) and (b) of this Regulation and shall impose on the data-subject the requirement to provide his or her fingerprints and a facial image <i>biometric data</i> and inform them them <i>him or her</i> as such in accordance with Article 30 of this Regulation. <i>Member States shall, at all times, respect the dignity and physical integrity of the person during the fingerprinting procedure and when capturing</i>	1. Member States are obliged to take the biometric data [...] of persons referred to in Article 10(1), 13(1) and 14(1) for the purposes of Article 1(1)(a) and (b) of this Regulation and shall impose on the data-subject the requirement to provide his or her biometric data [...] and inform them as such in accordance with Article 30 of this Regulation.	<i>Confirmed by trilogue (pending agreement on reference to the Article on resettled persons' data)</i> 1. Member States are obliged to take the biometric data [...] of persons referred to in Article 10(1), [12a] , 13(1) and 14(1) for the purposes of Article 1(1)(a), [1(aa)] and (b) of this Regulation and shall impose on <i>those persons</i> the requirement to provide <i>their biometric data</i> [...] and inform them in accordance with Article 30 of this Regulation. <i>(Last sentence of EP text moved to next paragraph)</i>


	<i>his or her facial image.</i>		
<p>2. Taking fingerprints and facial images of minors from the age of six shall be carried out in a child-friendly and child-sensitive manner by officials trained specifically to enrol minor's fingerprints and facial images. The minor shall be informed in an age-appropriate manner using leaflets and/or infographics and/or demonstrations specifically designed to explain the fingerprinting and facial image procedure to minors and they shall be accompanied by a responsible adult, guardian or representative at the time their fingerprints and facial image are taken. At all times Member States must respect the dignity and physical integrity of the minor during the fingerprinting procedure and when capturing a facial image.</p>	<p>Amendment 40</p> <p>2. Taking fingerprints and facial images of minors from the age of six shall be carried out in a child-friendly and child-sensitive manner by officials trained specifically to enrol minor's fingerprints and facial images. The minor shall be informed in an age-appropriate manner using leaflets and/or infographics and/or demonstrations specifically designed to explain the fingerprinting and facial image procedure to minors and they shall be accompanied by a responsible adult, guardian or representative at the time their fingerprints and facial image are taken. At all times Member States must respect the dignity and physical integrity of the minor during the fingerprinting procedure and when capturing a facial image.</p>	<p>2. Taking biometric data [...] of minors from the age of six shall be carried out in a child-friendly and child-sensitive manner by officials trained specifically to enrol minor's fingerprints and to capture facial images. [...] Minors shall be accompanied by a responsible adult, [guardian or legal representative] at the time their biometric data [...] are taken. At all times Member States must respect the dignity and physical integrity of the minor during the fingerprinting procedure and when capturing a facial image.</p>	<p><i>Confirmed by trilogue</i></p> <p>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.</p>
<p>3. Member States may introduce administrative sanctions, in accordance with their national law, for non-compliance with the fingerprinting process and capturing a facial image in</p>	<p>Amendment 41</p> <p>3. In order to ensure that all the persons referred to in Articles 10(1), 13(1) and 14(1) are registered in accordance with</p>	<p>3. Member States shall [...] introduce administrative sanctions including the possibility to use means of coercion, in accordance with their national law, for non-compliance with providing</p>	<p><i>Under discussion (see also recitals 30 and 30a and Art. 30(1)(d))</i></p> <p>3. Administrative measures for ensuring compliance with providing biometric data in accordance with</p>


<p>accordance with paragraph 1 of this Article. These sanctions shall be effective, proportionate and dissuasive. In this context, detention should only be used as a means of last resort in order to determine or verify a third-country national's identity.</p>	<p>paragraph 1, Member States may introduce, <i>where appropriate, well-justified</i> administrative sanctions, in accordance with their national law <i>and with full respect for the Charter of Fundamental Rights of the European Union</i>, for non-compliance with the fingerprinting process and capturing a facial image in accordance with paragraph 1 of this Article. These sanctions process <i>of taking biometric data</i>. <i>Member States shall ensure that an opportunity for counselling has been provided to those persons in order to persuade them to cooperate with the procedure and to inform them of the possible implications of non-compliance. The administrative sanctions</i> shall be effective, proportionate and dissuasive. In this context, detention should <i>Detention shall</i> only be used as a means of last resort <i>and for as short a period as possible and necessary</i> in order to determine or verify a third-country national's identity <i>and, in particular, where there is a risk of absconding. Where a decision is taken to detain a third-country national or a stateless person, competent</i></p>	<p>biometric data [...] in accordance with paragraph 1 of this Article. These sanctions shall be effective, proportionate and dissuasive. [...]</p>	<p>paragraph 1 of this Article <i>shall</i> be laid down in national law. These measures shall be effective, proportionate and dissuasive [<i>and may include the possibility to use means of coercion as a last resort.</i>]</p>
---	---	--	---

	<i>national authorities shall carry out an assessment in each individual case in order to verify whether the detention complies with all legal and procedural safeguards to prevent arbitrary detention.</i>		
4. Without prejudice to paragraph 3 of this Article, where enrolment of the fingerprints or facial image is not possible from third-country nationals who are deemed to be vulnerable persons and from a minor due to the conditions of the fingertips or face, the authorities of that Member State shall not use sanctions to coerce the taking of fingerprints or a facial image. A Member State may attempt to re-take the fingerprints or facial image of a minor or vulnerable person who refuses to comply, where the reason for non-compliance is not related to the conditions of the fingertips or facial image or the health of the individual and where it is duly justified to do so. Where a minor, in particular an unaccompanied or separated minor refuses to give their fingerprints or a facial image and there are reasonable grounds to suspect that	Amendment 42 4. Without prejudice to paragraph 3 of this Article, where enrolment of the fingerprints or facial image is not possible from third-country nationals <i>or stateless persons</i> who are deemed to be vulnerable persons and from a minor due to the conditions of the fingertips or face, the authorities of that Member State shall not use sanctions to coerce the taking of fingerprints or a facial image for <i>non-compliance with the obligation to provide biometric data</i> . A Member State may attempt to re-take the fingerprints or facial image of a vulnerable person who refuses to comply, where the reason for non-compliance is not related to the conditions of the fingertips or facial image or the health of the individual and where it is duly justified to do so. Where a minor,	4. Without prejudice to paragraph 3 of this Article, where enrolment of biometric data [...] is not possible from third-country nationals or stateless persons who are deemed to be vulnerable persons and from a minor due to the conditions of the fingertips or face, the authorities of that Member State shall not use sanctions to coerce the taking of biometric data [...]. A Member State may attempt to re-take the biometric data [...] of a minor or vulnerable person who refuses to comply, where the reason for non-compliance is not related to the conditions of the fingertips or facial image or the health of the individual and where it is duly justified to do so. Where a minor, in particular an unaccompanied or separated minor refuses to give their biometric data [...] and there are reasonable grounds to suspect that there are child	<i>Informal outcome of technical discussion (last sentence in the Council text moved to Art. 2a(2))</i> 4. Without prejudice to paragraph 3 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, <u>due to the condition of that person's fingertips or face, and where that person did not intentionally bring about the condition</u> , the authorities of that Member State <i>shall not employ administrative measures for ensuring compliance with the obligation to provide</i> biometric data. A Member State may attempt to re-take the biometric data [...] of a vulnerable person who refuses to comply, where the reason for non-compliance is not related to the conditions of the fingertips or facial image or the health of the individual

there are child safeguarding or protection risks, the minor shall be referred to the national child protection authorities and /or national referral mechanisms.	in particular an unaccompanied or separated minor refuses to give their fingerprints or a facial image and there are reasonable grounds to suspect that there are child safeguarding or protection risks, the minor shall be referred to the national child protection authorities and /or national referral mechanisms.	safeguarding or protection risks, the minor shall be referred to the national child protection authorities and /or national referral mechanisms.	and where it is duly justified to do so.
5. The procedure for taking fingerprints \Rightarrow and a facial image \Leftarrow shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child.	Amendment 43 5. The procedure for taking fingerprints and a facial image shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union and in the Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child.	5. The procedure for taking biometric data [...] shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child.	<i>Confirmed by trilogue</i> 5. The procedure for taking biometric data [...] shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms.

	Amendment 44 <i>Article 2a</i>		
	<i>Special provisions relating to minors</i>		
	<p><i>1. The biometric data of minors from the age of six shall be taken by officials trained specifically to enrol minor's fingerprints and to capture facial images in full respect of the best interests of the child, the principles established by the United Nations Convention on the Rights of the Child in a child-friendly and child-appropriate and gender-appropriate manner. The minor shall be informed in an age-appropriate manner, both orally and in writing, using leaflets and infographics and demonstrations specifically designed to explain the fingerprinting and facial image procedure to minors in a language he or she can understand. The minor shall be accompanied by a responsible adult or legal guardian throughout the time his or her biometric data are taken. At all times Member States shall respect the dignity and physical integrity</i></p>		<p><i>Informal outcome of technical discussion pending square bracketed provisions - see also Article 30(2) second subparagraph</i></p> <p><i>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.</i></p> <p><i>The minor shall be accompanied by [a responsible adult, guardian or legal representative]/ [family member or guardian] throughout the time his or her biometric data are taken.</i></p> <p><i>Rapporteur's proposal</i></p> <p><i>[Member States shall not use coercive administrative measures to obtain biometric data from minors.]</i></p>

	<p><i>of the minor during the fingerprinting procedure and when capturing a facial image. Member States shall not use coercion to compel the taking of fingerprints of minors. Detention of minors shall be prohibited.</i></p>		<p><i>Presidency compromise proposal - alternative 1:</i></p> <p>Minors should not be coerced into giving their biometric data, except in duly justified circumstances that are permitted under national law and where, taking into account the age and maturity of the minor, certain degree of coercion is considered appropriate.</p> <p><i>alternative 2:</i></p> <p>Member States shall not use force to compel the taking of biometric data of minors.</p>
	<p><i>2. Where the enrolment of the fingerprints or facial image of a minor is not possible due to the conditions of the fingertips or face, Article 2(3) 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 his or her fingerprints or a facial image and there are reasonable grounds for believing that there are child</i></p>		<p><i>Confirmed by trilogue</i></p> <p><i>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(4) 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</i></p>

	<p><i>safeguarding or protection risks, as assessed by an official trained specifically to deal with minors, the minor shall be referred to the competent national child protection authorities, the national referral mechanisms or both.</i></p>		<p>for believing that there are child safeguarding or protection risks, as assessed by <i>an official trained specifically to take a minor's biometric data</i>, the minor shall be referred to the competent national child protection authorities, the national referral mechanisms or both.</p>
--	--	---	--

	<p>3. For the purposes laid down in Article 13(1) and Article 14(1), each set of data relating to a minor shall be stored in the Central System for five years from the date on which his or her biometric data were taken.</p>		<p>Confirmed by trilogue</p> <p>Deletion</p>
	<p>4. Without prejudice to national criminal law, in particular relating to the age of criminal responsibility, where a request under Article 1(1)(c) concerns the data of a minor, it shall be accompanied by evidence of the relevance of those data for the prevention, detection or investigation of child trafficking or other serious crimes against children.</p>		<p>Confirmed by trilogue</p> <p>Deletion</p>
	<p>5. Member States shall record in the Schengen Information System (SIS) the biometric data of children who have gone missing from reception facilities as missing persons. Missing children identified by Member States' law enforcement authorities based on a hit pursuant to Article 26 of this Regulation shall be promptly referred to the competent national child protection authorities, which shall undertake a needs</p>		<p>Confirmed by trilogue</p> <p>Deletion (link to recital 25)</p>

	<i>assessment with a view to finding a sustainable solution for the child in accordance with his or her best interests.</i>		
<i>Article 2 3</i>		<i>Article 3</i>	
Definitions		Definitions	
1. For the purposes of this Regulation:			
(a) 'applicant for international protection' means a third-country national or a stateless person who has made an application for international protection as defined in Article 2(h) of Directive 2011/95/EU in respect of which a final decision has not yet been taken;			
	<p>Amendment 45</p> <p><i>(aa) 'resettled third-country national or stateless person' means a third-country national or stateless person who, following a resettlement procedure in accordance with national law or with [Regulation XXX/XXX], arrives on the territory of the Member State of resettlement.</i></p>		<i>The Council does not have a mandate yet to discuss this text with the EP.</i>

(b) 'Member State of origin' means:			
(i) in relation to a person covered by Article 9 10(1), the Member State which transmits the personal data to the Central System and receives the results of the comparison;			
	Amendment 46 <i>(ia) in relation to a person covered by Article 12a, the Member State which transmits the personal data to the Central System and receives the results of the comparison;</i>		<i>The Council does not have a mandate yet to discuss this text with the EP.</i>
(ii) in relation to a person covered by Article 14 13(1), the Member State which transmits the personal data to the Central System ⇒ and receives the results of the comparison ⇐ ;			
(iii) in relation to a person covered by Article 17 14(1), the Member State which transmits the personal data to the Central System and receives the results of the comparison;			
(c) 'third-country national'		(c) 'third-country national'	(c) 'third-country national' means

means any person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty and who is not a national of a State which participates in this Regulation by virtue of an agreement with the European Union;		means any person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty and who is not a national of a State which participates in this Regulation by virtue of an agreement with the [...] Union;	any person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty and who is not a national of a State which participates in this Regulation by virtue of an agreement with the Union;
(d) 'illegal stay' means the presence on the territory of a Member State, of a third-country national who does not fulfil, or no longer fulfils the conditions of entry as set out in Article 5 of the Schengen Borders Code or other conditions for entry, stay or residence in that Member State;	Amendment 47 (d) 'illegal stay' means the presence on the territory of a Member State, of a third-country national or stateless person who does not fulfil, or no longer fulfils the conditions of entry as set out in Article 5 of the Schengen Borders Code or other conditions for entry, stay or residence in that Member State;	(d) 'illegal stay' means the presence on the territory of a Member State, of a third-country national or a stateless person who does not fulfil, or no longer fulfils the conditions of entry as set out in Article 5 of the Schengen Borders Code or other conditions for entry, stay or residence in that Member State;	(d) 'illegal stay' means the presence on the territory of a Member State, of a third-country national or a stateless person who does not fulfil, or no longer fulfils the conditions of entry as set out in Article 5 of the Schengen Borders Code or other conditions for entry, stay or residence in that Member State;
(ee) 'beneficiary of international protection' means a third-country national or a stateless person who has been granted international protection as defined in Article 2(a) of Directive 2011/95/EU;			
(ef) 'hit' means the existence of a match or matches established by the Central System by comparison between fingerprint data recorded in the computerised central database and those transmitted by	Amendment 48 (f) 'hit' means the existence of a match or matches established by the Central System by comparison between fingerprint biometric data	(f) 'hit' means the existence of a match or matches established by the Central System by comparison between biometric [...] data recorded in the computerised central database and those	(f) 'hit' means the existence of a match or matches established by the Central System by comparison between biometric data recorded in the computerised central database and those transmitted by a Member State

a Member State with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 25 26(4);	recorded in the computerised central database and those transmitted by a Member State with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 26(4);	transmitted by a Member State with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 26(4);	with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 26(4);
(eg) 'National Access Point' means the designated national system which communicates with the Central System;			
			<i>(ga) 'Europol Access Point' means the designated Europol system which communicates with the Central System</i>
(fh) 'Agency' <input checked="" type="checkbox"/> 'eu-LISA' <input checked="" type="checkbox"/> means the <input checked="" type="checkbox"/> European <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> for the operational management of large-scale information systems in the area of freedom, security and justice <input checked="" type="checkbox"/> established by Regulation (EU) No 1077/2011;			
(gi) 'Europol' means the European Police Office established by Decision 2009/371/JHA;		(i) 'Europol' means the European Police Office established by Regulation (EU) 2016/794 [...];	(i) 'Europol' means the European Police Office established by Regulation (EU) 2016/794 ;


<p>(hi) 'Eurodac data' means all data stored in the Central System in accordance with Article 11 12, and Article 14 13(2) ⇒ and Article 14(2) ⇐ ;</p>	<p>Amendment 49</p> <p>(j) 'Eurodac data' means all data stored in the Central System in accordance with Article 12, Article 12a, Article 13(2) and Article 14(2);</p>	<p><i>Text agreed with the exception of the reference to the Article on resettled persons' data</i></p> <p>(j) 'Eurodac data' means all data stored in the Central System in accordance with Article 12, Article [12a], Article 13(2) and Article 14(2);</p>
<p>(k) 'law enforcement' means the prevention, detection or investigation of terrorist offences or of other serious criminal offences;</p>	<p>Amendment 50</p> <p>(k) 'law enforcement' means the prevention, detection, or investigation or prosecution of terrorist offences or of other serious criminal offences; <i>(This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.)</i></p>	<p><i>Confirmed by trilogue</i></p> <p>(k) 'law enforcement' means the prevention, detection or investigation of terrorist offences or of other serious criminal offences;</p>
<p>(l) 'terrorist offences' means the offences under national law which correspond or are equivalent to those referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA;</p>	<p>Amendment 51</p> <p>(l) 'terrorist offences' means the offences under national law which correspond or are equivalent to those referred to in Articles 1 to 4 of referred to in Articles 3 to 12 of Directive (EU) 2017/... of the European Parliament and of the Council [on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision</p>	<p><i>Confirmed by trilogue</i></p> <p>(l) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences referred to in Directive (EU) 2017/541;</p>


	2005/671/JHAJ.		
(k m) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA, if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;			
(h n) 'fingerprint data' means the data relating to ⇒ plain and rolled impressions of the ⇐ fingerprints of all ⇐ ten fingers, where present ⇐ or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent fingerprint ;			
(o) facial image means digital images of the face with sufficient image resolution and quality to be used in automatic biometric matching.		(o) 'facial image data ' means digital images of the face with sufficient image resolution and quality to be used in automatic biometric matching;	(o) 'facial image data ' means digital images of the face with sufficient image resolution and quality to be used in automatic biometric matching;
	Amendment 52 (oa) <i>'biometric data' means fingerprint data and facial image data;</i> (This amendment applies throughout the text. Adopting it	(p) 'biometric data' means fingerprint data and facial image data for the purposes of this Regulation;	(p) 'biometric data' means fingerprint data and facial image data for the purposes of this Regulation;

	<i>will necessitate corresponding changes throughout.)</i>		
	Amendment 53 <i>(ob) 'stateless person' means a person who is not considered to be a national of any State under the operation of its law.</i>		<i>Confirmed by trilogue</i> <i>Deletion</i>
	Amendment 54 <i>(oc) 'alphanumeric data' means data represented by letters, digits, special characters, spaces and punctuation marks;</i>	(q) 'alphanumeric data' means data represented by letters, digits, special characters, space and punctuation marks;	(q) 'alphanumeric data' means data represented by letters, digits, special characters, space and punctuation marks;
	Amendment 55 <i>(od) 'residence document' means a residence document as defined in point (...) of Article of Regulation ... [COD(2016)0133; Dublin IV];</i>	(r) '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) No XXX/XXX	(r) '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) No XXX/XXX [Dublin Regulation] or

		[Dublin Regulation] or during the examination of an application for international protection or an application for a residence permit;	during the examination of an application for international protection or an application for a residence permit;
	Amendment 56 <i>(oe) 'interface control document' means a technical document that specifies the necessary requirements with which the national access points referred to in Article 4(3) are to comply in order to be able to communicate electronically with the Central System, in particular by detailing the form and possible content of the information to be exchanged between the Central System and the national access points.</i>	(s) 'Interface Control Document' means the technical document that specifies the necessary requirements to which the National Access Points must adhere, to be able to communicate electronically with the Central system, in particular by detailing the format and possible content of the information exchanged between the Central system and the National Access Points.	<i>Confirmed by trilogue</i> <i>(oe) '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 the Central System, in particular by detailing the format and possible content of the information to be exchanged between the Central System and the National or the Europol access points.</i>
2. The terms defined in Article [..] 2 of Directive [2016/.../EU] 95/46/EC shall have the same meaning in this Regulation in so far as personal data are processed by the authorities of the Member States for the purposes laid down in Article 1(1)(a) of this Regulation.		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.	<i>Confirmed by trilogue</i> 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		3. Unless stated otherwise, the terms defined in Article 2 of	<i>Confirmed by trilogue</i>

Regulation (EU) No 604/2013 [...] shall have the same meaning in this Regulation.		Regulation (EU) No XXX/XXX [Dublin Regulation] [...] shall have the same meaning in this Regulation.	3. Unless stated otherwise, the terms defined in Article 2 of Regulation (EU) No XXX/XXX [Dublin Regulation] shall have the same meaning in this Regulation.
4. The terms defined in Article [...] 2 of Directive [2016/.../EU] Framework Decision 2008/977/JHA shall have the same meaning in this Regulation in so far as personal data are processed by the <input checked="" type="checkbox"/> competent <input checked="" type="checkbox"/> authorities of the Member States for the purposes laid down in Article 1 (2) (1)(c) of this Regulation.		4. The terms defined in Article 3 of Directive (EU) 2016/680 [...] shall have the same meaning in this Regulation in so far as personal data are processed by the competent authorities of the Member States for the purposes laid down in Article 1(1)(c) of this Regulation.	<i>Confirmed by trilogue</i> 4. The terms defined in Article 3 of Directive (EU) 2016/680 shall have the same meaning in this Regulation in so far as personal data are processed by the competent authorities of the Member States for the purposes laid down in Article 1(1)(c) of this Regulation.
<i>Article 3 4</i>		<i>Article 4</i>	
System architecture and basic principles		System architecture and basic principles	
1. Eurodac shall consist of:			
(a) a computerised central fingerprint database ("Central System") composed of:		(a) a [...] Central System [...] composed of:	(a) a Central System composed of:
(i) a Central Unit,			
(ii) a Business Continuity Plan and System;			

<p>(b) a communication infrastructure between the Central System and Member States that provides an encrypted virtual network dedicated to ⇒ a secure and encrypted communication channel for ⇐ Eurodac data ("Communication Infrastructure").</p>			
<p>2. The EURODAC Communication Infrastructure will be using the existing 'Secure Trans European Services for Telematics between Administrations' (TESTA) network. A separate virtual private network dedicated to the EURODAC shall be established on the existing TESTA private virtual network to ensure the logical separation of EURODAC data from other data.</p>	<p>Amendment 57</p> <p>2. The EURODAC Communication Infrastructure will be using the existing 'Secure Trans European Services for Telematics between Administrations' (TESTA) network. A separate virtual private network dedicated to the EURODAC shall be established on the existing TESTA private virtual network to ensure the logical separation of EURODAC data from other data <i>In order to ensure confidentiality, personal data transmitted to or from Eurodac shall be encrypted.</i></p>	<p>2. The EURODAC Communication Infrastructure will be using the existing 'Secure Trans European Services for Telematics between Administrations' (TESTA ng) network. In order to ensure confidentiality, personal data transmitted to or from Eurodac shall be encrypted. [...]</p>	<p><i>Confirmed by trilogue</i></p> <p>2. 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. [...]</p>
<p><u>23.</u> Each Member State shall have a single National Access Point.</p>	<p>Amendment 58</p> <p>3. Each Member State shall have a single National Access Point. <i>Europol shall have its own access point.</i></p>		<p><i>Confirmed by trilogue</i></p> <p>Each Member State shall have a single National Access Point. Europol shall have a single Europol access point.</p>

<p>34. Data on persons covered by Articles 9 10(1), 14 13(1) and 17 14(1) which are processed in the Central System shall be processed on behalf of the Member State of origin under the conditions set out in this Regulation and separated by appropriate technical means.</p>	<p>Amendment 59</p> <p>4. Data on persons covered by Articles 10(1), 12a, 13(1) and 14(1) which are processed in the Central System shall be processed on behalf of the Member State of origin under the conditions set out in this Regulation and separated by appropriate technical means.</p>		<p><i>Text agreed with the exception of the reference to the Article on resettled persons' data</i></p> <p>4. Data on persons covered by Articles 10(1), [12a,] 13(1) and 14(1) which are processed in the Central System shall be processed on behalf of the Member State of origin under the conditions set out in this Regulation and separated by appropriate technical means.</p>
<p>45. The rules governing Eurodac shall also apply to operations carried out by the Member States as from the transmission of data to the Central System until use is made of the results of the comparison.</p>			
<p><i>Article 4 5</i></p>		<p><i>Article 5</i></p>	
<p>Operational management</p>		<p>Operational management</p>	
<p>1. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall be responsible for the operational management of Eurodac.</p>			
<p>The operational management of Eurodac shall consist of all the tasks necessary to keep Eurodac</p>			

functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System. A Business Continuity Plan and System shall be developed taking into account maintenance needs and unforeseen downtime of the system, including the impact of business continuity measures on data protection and security.			
The Agency ☒ 2. eu-LISA ☒ shall ensure, in cooperation with the Member States, that at all times the best available and most secure technology and techniques, subject to a cost-benefit analysis, are used for the Central System.			
2. Eu-LISA shall be permitted to use real personal data of the Eurodac production system for testing purposes in the following circumstances:	Amendment 60 Eu-LISA shall be permitted to use real personal data of the Eurodac production system for testing purposes, <i>in accordance with Regulation (EU) 2016/679, and in</i>		<i>Confirmed by trilogue</i> 2. Eu-LISA shall be permitted to use real personal data of the Eurodac production system for testing purposes, <i>in accordance with Regulation (EU) 2016/679, in the</i>

	<i>strict compliance with Article 17 of the Staff Regulations⁵¹ in respect of every person involved in the testing only</i> in the following circumstances:		following circumstances:
(a) for diagnostics and repair when faults are discovered with the Central System; and			
(b) for testing new technologies and techniques relevant to enhance the performance of the Central System or transmission of data to it.			
In such cases, the security measures, access control and logging activities at the testing environment shall be equal to the ones for the Eurodac production system. Real personal data adopted for testing shall be rendered anonymous in such a way that the data-subject is no longer identifiable.	<p>Amendment 61</p> <p>In such cases, the security measures, access control and logging activities at the testing environment shall be equal to the ones for the Eurodac production system. Real personal data adopted for testing shall be <i>subject to stringent conditions and</i> rendered anonymous in such a way that the data-subject is no longer identifiable. <i>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</i></p>	In such cases, the security measures, access control and logging activities at the testing environment shall be equal to the ones for the Eurodac production system. Real personal data adopted for testing shall be rendered anonymous in such a way that the data-subject is no longer identifiable, where such data can be anonymised.	<p><i>Confirmed by trilogue</i></p> <p>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. <i>Processing of</i> real personal data <i>adapted</i> for testing shall be <i>subject to stringent conditions and</i> rendered anonymous in such a way that the data-subject is no longer identifiable. <i>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.</i></p>

⁵¹ Council Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union (OJ L 56, 4.3.1968, p.1).

	<i>environment. Eu-LISA shall ensure that relevant guarantees are provided in respect of the accessing of data by external contractors, in accordance with Articles 24 to 28 of Regulation (EU) 2016/679.</i>		
23. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> 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.			
	Amendment 62 <i>(ca) interoperability with other information systems.</i>		<i>Confirmed by trilogue</i> Deletion
34. The Commission shall be responsible for all tasks relating to the Communication Infrastructure other than those referred to in paragraph 2 <u>3</u> , in particular:			
(a) the implementation of the budget;			

(b) acquisition and renewal;			
(c) contractual matters.			
5. A separate secure electronic transmission channel between the authorities of Member States known as the 'DubliNet' communication network set-up under [Article 18 of Regulation (EC) No. 1560/2003] for the purposes set out in Articles 32, 33 and 46 of Regulation (EU) No. [...] shall also be operated and managed by eu-LISA.		5. [...]	5. <i>deleted (new Article 40a para. 1)</i>
46. Without prejudice to Article 17 of the Staff Regulations, the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> 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.			
<i>Article 5 6</i>		<i>Article 6</i>	
Member States' designated authorities for law enforcement		Member States' designated authorities for law enforcement	


purposes		purposes	
<p>1. For the purposes laid down in Article 1(2)(1)(c), Member States shall designate the authorities that are authorised to request comparisons with Eurodac data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security.</p>	<p>Amendment 63</p> <p>1. For the purposes laid down in Article 1(1)(c), Member States shall designate the authorities that are authorised to request comparisons with Eurodac data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security.</p>	<p>1. For the purposes laid down in Article 1(1)(c), Member States shall designate the authorities that are authorised to request comparisons with Eurodac data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. [...]</p>	<p>1. For the purposes laid down in Article 1(1)(c), Member States shall designate the authorities that are authorised to request comparisons with Eurodac data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.</p>
<p>2. Each Member State shall keep a list of the designated authorities.</p>	<p>Amendment 64</p> <p>2. Each Member State shall keep a list of the designated authorities <i>and communicate it without delay to the Commission and to eu-LISA. Eu-LISA shall publish a consolidated list of those designated authorities in the Official Journal of the European Union. Where that list has been amended, eu-LISA shall annually publish an updated</i></p>		<p><i>Confirmed by trilogue</i></p> <p>2. Each Member State shall keep a list of the designated authorities.</p>

	<i>consolidated list online.</i>		
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.			
<i>Article 6 7</i>		<i>Article 7</i>	
Member States' verifying authorities for law enforcement purposes		Member States' verifying authorities for law enforcement purposes	
1. For the purposes laid down in Article 1(2)(1)(c), each Member State shall designate a single national authority or a unit of such an authority to act as its verifying authority. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.			
The designated authority and the verifying authority may be part of the same organisation, if permitted under national law, but the verifying authority shall act independently when performing its			

tasks under this Regulation. The verifying authority shall be separate from the operating units referred to in Article 5 6(3) and shall not receive instructions from them as regards the outcome of the verification.			
Member States may designate more than one verifying authority to reflect their organisational and administrative structures, in accordance with their constitutional or legal requirements.			
2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with Eurodac data are fulfilled.	Amendment 65 The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints biometric or alphanumeric data with Eurodac data are fulfilled.	2. The verifying authority shall ensure that the conditions for requesting comparisons of biometric or alphanumeric data [...] with Eurodac data are fulfilled.	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 19 20.			
Only the verifying authority shall be authorised to forward requests for comparison of fingerprints ⇨ and facial images ⇧ to the	Amendment 66 Only the verifying authority shall be authorised to forward requests	Only the verifying authority shall be authorised to forward requests for comparison of biometric or alphanumeric data [...] to the	Only the verifying authority shall be authorised to forward requests for comparison of biometric or alphanumeric data to the National

National Access Point.	for comparison of fingerprints and facial images biometrics or alphanumeric data to the National Access Point.	National Access Point.	Access Point.
<i>Article 7 8</i>		<i>Article 8</i>	
Europol		Europol	
<p>1. For the purposes laid down in Article 1(2)(1)(c), Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority, which shall act independently of the designated authority referred to in paragraph 2 of this Article when performing its tasks under this Regulation and shall not receive instructions from the designated authority as regards the outcome of the verification. The unit shall ensure that the conditions for requesting comparisons of fingerprints ⇨ and facial images ⇨ with Eurodac data are fulfilled. Europol shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint ⇨ and facial image ⇨ data to the Central</p>	<p>Amendment 67</p> <p>1. For the purposes laid down in Article 1(1)(c), Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority, which shall act independently of the designated authority referred to in paragraph 2 of this Article when performing its tasks under this Regulation and shall not receive instructions from the designated authority as regards the outcome of the verification. The unit shall ensure that the conditions for requesting comparisons of fingerprints and facial images with Eurodac data are fulfilled. Europol shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint and facial image data</p>	<p>1. For the purposes laid down in Article 1(1)(c), Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority, which shall act independently of the designated authority referred to in paragraph 2 of this Article when performing its tasks under this Regulation and shall not receive instructions from the designated authority as regards the outcome of the verification. The unit shall ensure that the conditions for requesting comparisons of biometric or alphanumeric data [...] with Eurodac data are fulfilled. Europol shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of biometric or alphanumeric [...] data to the</p>	<p><i>Confirmed by trilogue</i></p> <p>1. For the purposes laid down in Article 1(1)(c), 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.</p>

System.	to the Central System <i>an authority which is authorised to request comparisons with Eurodac data through its designated Europol access point in order to prevent, detect and investigate terrorist offences or other serious criminal offences.</i> The <i>designated authority</i> shall <i>be an operating unit of Europol.</i>	Central System.	
2. For the purposes laid down in Article 1(2) (1)(c), Europol shall designate an operating unit that is authorised to request comparisons with Eurodac data through its designated National Access Point. The designated authority shall be an operating unit of Europol which is competent to collect, store, process, analyse and exchange information to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling within Europol's mandate.	Amendment 68 2. For the purposes laid down in Article 1(1)(c), Europol shall designate an <i>operating specialised</i> unit that is authorised to request comparisons with Eurodac data through its designated National Access Point. The designated authority shall be an operating unit of Europol which is competent to collect, store, process, analyse and exchange information to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling within Europol's mandate. <i>with duly empowered Europol officials as the Europol access point. The Europol access point shall verify that the conditions to request comparisons with</i>		<i>Confirmed by trilogue</i> 2. For the purposes laid down in Article 1(1)(c), Europol shall designate a single specialised unit with duly empowered Europol officials to act as its verifying authority which shall be authorised to <i>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.</i> The verifying authority shall ensure that the conditions for

	<i>Eurodac data laid down in Article 22 are fulfilled. The Europol access point shall act independently when performing its tasks under this Regulation and shall not receive instructions from the designated authority referred to in paragraph 1 as regards the outcome of the verification.</i>		requesting comparisons of biometric or alphanumeric data with Eurodac data are fulfilled.
	<p>Amendment 69</p> <p><i>2 a. Europol shall designate an operating unit in charge of collecting, storing, processing, analysing and exchanging the data on child victims of trafficking in human beings. The operating unit shall be authorised to request comparisons with Eurodac data in order to support and strengthen Member States' action in preventing, detecting or investigating child trafficking, child labour or sexual exploitation.</i></p>		<p><i>Confirmed by trilogue</i></p> <p><i>Deletion + new recital 38a</i></p>

	Amendment 70 <i>Article 8 a</i>		
	<i>European Border and Coast Guard</i>		
	<i>In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the European Border and Coast Guard Agency or teams of staff involved in return-related tasks as well as the members of the migration management support teams shall, within their mandate, have the right to access and search data entered in Eurodac. They shall access the data by using the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to in Article 10(3a) of this Regulation.</i>		Confirmed by trilogue Deletion + recitals (13a) and (13b)
<i>Article 8 9</i>		<i>Article 9</i>	
Statistics		Statistics	
1. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall draw up statistics on the work of the Central System every <input checked="" type="checkbox"/> month <input checked="" type="checkbox"/> quarter, indicating in particular:			

(a) the number of data sets transmitted on persons referred to in Articles 9 10(1), 14 13(1) and 17 14(1);	Amendment 71 (a) the number of data sets transmitted on persons referred to in Articles 10(1), 12a , 13(1) and 14(1);		<i>Text agreed with the exception of the reference to the Article on resettled persons' data</i> (a) the number of data sets transmitted on persons referred to in Articles 10(1), [12a] , 13(1) and 14(1);
(b) the number of hits for applicants for international protection <input checked="" type="checkbox"/> persons referred to in Article 10(1) <input checked="" type="checkbox"/> who have <input checked="" type="checkbox"/> subsequently <input checked="" type="checkbox"/> lodged an application for international protection in another Member State <input checked="" type="checkbox"/> , who were apprehended in connection with the irregular crossing of an external border and who were found illegally staying in a Member State <input checked="" type="checkbox"/> ;		(b) the number of hits for persons referred to in Article 10(1);	Restructured provision (see also points i,ii,iii) (b) the number of hits for persons referred to in Article 10(1);
		(i) who have subsequently lodged an application for international protection in another Member State,	(i) who have subsequently lodged an application for international protection in another Member State,
		(iii) who were apprehended in connection with the irregular crossing of an external border, and	(ii) who were apprehended in connection with the irregular crossing of an external border, and
		(iv) who were found illegally staying in a Member State;	(iii) who were found illegally staying in a Member State;
(c) the number of hits for		(c) the number of hits for	(c) the number of hits for persons

persons referred to in Article 14 13(1) who have subsequently lodged an application for international protection ⇒ who were apprehended in connection with the irregular crossing of an external border and who were found illegally staying in a Member State ⇐ ;		persons referred to in Article 13(1):	referred to in Article 13(1):
		(i) who have subsequently lodged an application for international protection,	(i) who have subsequently lodged an application for international protection,
		(iii) who were apprehended in connection with the irregular crossing of an external border, and	(ii) who were apprehended in connection with the irregular crossing of an external border, and
		(iv) who were found illegally staying in a Member State;	(iii) who were found illegally staying in a Member State;
(d) the number of hits for persons referred to in Article 17 14(1) who had previously lodged an application for international protection in another Member State ⇒ , who were apprehended in connection with the irregular crossing of an external border and who were found illegally staying in a Member State ⇐ ;		(d) the number of hits for persons referred to in Article 14(1):	(d) the number of hits for persons referred to in Article 14(1):
		(i) who had previously lodged an application for international protection in another Member	(i) who had previously lodged an application for international

		State,	protection in another Member State,
		(iii) who were apprehended in connection with the irregular crossing of an external border, and	(iii) who were apprehended in connection with the irregular crossing of an external border, and
		(iv) who were found illegally staying in a Member State;	(iv) who were found illegally staying in a Member State;
(e) the number of fingerprint data which the Central System had to request more than once from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;	Amendment 72 (e) the number of fingerprint biometric data which the Central System had to request more than once from the Member States of origin because the fingerprint biometric data originally transmitted did not lend themselves to comparison using the computerised fingerprint biometric recognition system;	(e) the number of biometric [...] data which the Central System had to request more than once from the Member States of origin because the biometric [...] data originally transmitted did not lend themselves to comparison using the computerised fingerprint and facial image recognition system;	<i>Confirmed by trilogue</i> (e) the number of biometric [...] data which the Central System had to request more than once from the Member States of origin because the biometric [...] data originally transmitted did not lend themselves to comparison using the computerised fingerprint and facial image recognition systems ;
(f) the number of data sets marked, unmarked, blocked and unblocked in accordance with Article 18 19(1) and (3) ⇒ 17(2), (3) and (4) ⇐ ;		(f) the number of data sets marked and [...] unmarked [...] in accordance with Article 19(1) and 19 [...] (2), (3) and (4);	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> (f) the number of data sets marked and unmarked in accordance with Article 19(1) and 19 (2), (3) and (4);
(g) the number of hits for persons referred to in Article 18 19(1) ⇒ and (4) ⇐ for whom hits have been recorded under points			

(b) ⇒, (c) ⇐ and (d) of this Article;			
(h) the number of requests and hits referred to in Article 20 21(1);			
(i) the number of requests and hits referred to in Article 21 22(1);			
(j) the number of requests made for persons referred to in Article 31;	Amendment 73 (j) the number <i>and type</i> of requests made for persons referred to in Article 31;		<i>Confirmed by trilogue</i> (j) the number of requests made for persons referred to in Article 31;
(h) the number of hits received from the Central System as referred to in Article 26(6).		(k) [...] the number of hits received from the Central System as referred to in Article 26(6).	(k) the number of hits received from the Central System as referred to in Article 26(6).
2. ⇒ The monthly statistical data for persons referred to in paragraph 1(a) to (h) shall be published and made public by each month. ⇐ At the end of each year, ☒ the yearly ☒ statistical data ⇒ for persons referred to in paragraph 1(a) to (h) ⇐ shall be ⇒ published and made public by eu-LISA ⇐ established in the form of a compilation of the quarterly statistics for that year, including an indication of the number of persons for whom hits have been recorded under paragraph 1(b), (c)	Amendment 74 2. The monthly statistical data for persons referred to in paragraph 1(a) to (h) shall contain a breakdown, where possible, of the data subjects' years of birth and genders, and shall be published and made public by each month. At the end of each year, the yearly statistical data for persons referred to in paragraph 1(a) to (h) shall be published and made public by eu-LISA. The statistics shall contain a	2. The monthly statistical data for persons referred to in paragraph 1(a) to (k) [...] shall be published and made public by each month. At the end of each year, the yearly statistical data for persons referred to in paragraph 1(a) to (k) [...] shall be published and made public by eu-LISA. The statistics shall contain a breakdown of data for each Member State.	<i>Confirmed by trilogue</i> 2. The monthly statistical data for persons referred to in paragraph 1(a) to (k) [...] shall be published each month. At the end of each year, the yearly statistical data for persons referred to in paragraph 1(a) to (k) [...] shall be published by eu-LISA. The statistical data shall be broken down by Member State. The statistical data for persons referred to in paragraph 1(a) shall, where possible, be broken down by year of

and (d). The statistics shall contain a breakdown of data for each Member State. The results shall be made public.	breakdown of data for each Member State.		birth and sex.
	<p>Amendment 75</p> <p><i>3 a. The duly authorised staff of the European Border and Coast Guard Agency shall have access to the statistics drawn up by eu-LISA referred to in points (a) to (h) of paragraph 1 of this Regulation and to the relevant data referred to in Article (12)(d) to (s), Article 13(2)(d) to (m) and Article 14(2)(d) to (m) of this Regulation, solely for the purposes laid down in Article 1(1)(b) of this Regulation and for the purposes laid down in Articles 11 and 37 of Regulation (EU) 2016/1624. Access shall be granted to such statistics and data in such a way as to ensure that individuals are not identified. The processing of those data shall be carried out in compliance with the data protection safeguards provided for in Regulation (EU) 2016/1624.</i></p>		<p><i>Confirmed by trilogue</i></p> <p><i>Deletion + recitals (13a) and (13b)</i></p>
3. At the request of the Commission, eu-LISA shall		3. At the request of the Commission, eu-LISA shall	<p><i>Confirmed by trilogue</i></p> <p>3. At the request of the</p>

provide it with statistics on specific aspects for research and analysis purposes without allowing for individual identification as well as the possibility to produce regular statistics pursuant to paragraph 1. These statistics shall be shared with other Justice and Home Affairs Agencies if they are relevant for the implementation of their tasks.		provide it with statistics on specific aspects related to the implementation of this Regulation as well as the statistics pursuant to paragraph 1, and make it available upon request to a Member State [...].	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.
		4. Eu-LISA shall establish, implement and host a central repository in its technical sites containing the data referred to in paragraphs 1 to 3, for research and analysis purposes, which would not allow for the identification of individuals and would allow the authorities listed in paragraph 5 to obtain customisable reports and statistics. Access to the central repository shall be granted by means of secured access through the TESTA-ng with control of access and specific user profiles solely for the purpose of reporting and statistics.	<i>Confirmed by trilogue</i> 4. Eu-LISA shall establish, implement and host a central repository in its technical sites containing the data referred to in paragraphs 1 to 3, for research and analysis purposes, which shall not allow for the identification of individuals and would allow the authorities listed in paragraph 5 to obtain customisable reports and statistics. The central repository shall only be accessible by means of a secured access through TESTA with control of access and specific user profiles solely for the purpose of reporting and statistics.
		5. Access to the central repository shall be granted to eu-	<i>Confirmed by trilogue</i>

		LISA, the Commission and to the authorities of Member States, which have been listed as the designated authorities responsible for carrying out tasks related to the application of this Regulation pursuant to Article 28(2). Access may also be granted to authorised users of other Justice and Home Affairs Agencies if access to the data hosted in the central repository is relevant for the implementation of their tasks.	5. Access to the central repository shall be granted to eu-LISA, to the Commission and to the authorities designated by each Member State in accordance with Article 28(2). Access may also be granted to authorised users of other Justice and Home Affairs Agencies if such access is relevant for the implementation of their tasks.
CHAPTER II		CHAPTER II	
<i>APPLICANTS FOR INTERNATIONAL PROTECTION</i>		APPLICANTS FOR INTERNATIONAL PROTECTION	
<i>Article 9 10</i>		<i>Article 10</i>	
Collection and comparison of fingerprints and facial image data		Collection and transmission of <u>biometric</u> [...] data	
1. Each Member State shall promptly take the fingerprints of all fingers ⇒ and capture a facial		1. Each Member State shall promptly take the biometric data [...] of every applicant for	1. Each Member State shall promptly take the biometric data of every applicant for international

<p>image of every applicant for international protection of at least 14 six years of age and shall, as soon as possible and no later than 72 hours after the lodging of his or her application for international protection, as defined by Article [21(2)]of Regulation (EU) No 604/2013, transmit them together with the data referred to in Article 11 12(b) to (g) (c) to (n) of this Regulation to the Central System.</p>		<p>international protection of at least six years of age and shall, as soon as possible and no later than 72 hours after the lodging of his or her application for international protection, as defined by [Article 21(2) of Regulation (EU) No XXX/XXX [Dublin Regulation] [...]], transmit them together with the data referred to in Article 12 (c) to (n) of this Regulation to the Central System.</p>	<p>protection of at least six years of age and shall, as soon as possible and no later than 72 hours after the lodging of his or her application for international protection, as defined by [Article 21(2) of Regulation (EU) No XXX/XXX [Dublin Regulation]], transmit them together with the data referred to in Article 12 (c) to (n) of this Regulation to the Central System.</p>
<p>Non-compliance with the 72-hour time-limit shall not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow the taking of the fingerprints of a quality ensuring appropriate comparison under Article 25 26, the Member State of origin shall retake the fingerprints of the applicant and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>		<p>Non-compliance with the 72-hour time-limit shall not relieve Member States of the obligation to take and transmit the biometric data [...] to the Central System. Where the condition of the fingertips does not allow the taking of the fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of the applicant and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>	<p>Non-compliance with the 72-hour time-limit shall not relieve Member States of the obligation to take and transmit the biometric data to the Central System. Where the condition of the fingertips does not allow the taking of the fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of the applicant and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>
<p>2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints</p>		<p>2. By way of derogation from paragraph 1, where it is not possible to take the biometric</p>	<p>2. By way of derogation from paragraph 1, where it is not possible to take the biometric data of an</p>

⇒ and facial image ⇐ of an applicant for international protection on account of measures taken to ensure his or her health or the protection of public health, Member States shall take and send such fingerprints ⇒ and facial image ⇐ as soon as possible and no later than 48 hours after those health grounds no longer prevail.		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.	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. Fingerprint data within the meaning of Article 11(a) transmitted by any Member State, with the exception of those transmitted in accordance with Article 10(b), shall be compared automatically with the fingerprint data transmitted by other Member States and already stored in the Central System.			
4. The Central System shall ensure, at the request of a Member State that the comparison referred to in paragraph 3 covers the fingerprint data previously			

transmitted by that Member State, in addition to the data from other Member States.			
5. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin. Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 11(a) to (k) along with, where appropriate, the mark referred to in Article 18(1).			
3. Fingerprint data may also be taken and transmitted by members of the European Border [and Coast] Guard Teams or by Member State asylum experts when performing tasks and exercising powers in accordance with [Regulation on the European Border [and Coast] Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC] and [Regulation (EU) No. 439/2010].	Amendment 76 3. Fingerprint <i>Where requested by the Member State concerned, the biometric</i> data may also be taken and transmitted by members of the European Border and Coast Guard Teams or by Member State asylum experts when performing tasks and exercising powers in accordance with [Regulation on the European Border [and Coast] Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision	3. Where requested by the Member State concerned, the biometric [...] data may also be taken and transmitted by members of the European Border and Coast Guard Teams or by Member State asylum experts when performing tasks and exercising powers in accordance with Regulation (EU) 2016/1624 of the European Parliament and of the Council [...] ⁵² and Regulation (EU) No. XXX/XXX [Regulation on the EU Agency for Asylum] [...].	<i>Confirmed by trilogue</i> <i>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) 2016/1624 and [Regulation (EU) No].</i>

⁵²

Regulation (EU) 2016/679 of the European Parliament and of 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).

	2005/267/EC] and [Regulation (EU) No. 439/2010] Regulation (EU) 2016/1624 or by asylum support teams in accordance with [Regulation (EU) No].		
	Amendment 77 <i>3a. For the purposes of paragraph 3, the European Border and Coast Guard Agency and the European Union Agency for Asylum established by Regulation (EU) 2017/... shall set up and maintain a technical interface which allows a direct connection to the Central System of Eurodac.</i>		Confirmed by trilogue Deletion + recitals (13a) and (13b)
Article 10 11		Article 11	
Information on the status of the data subject		Information on the status of the data subject	
The following information shall be sent to the Central System in order to be stored in accordance with Article 12 17 (1) for the purpose of transmission under Articles 9(5) ⇒ 15 and 16 ⇐ :			
		[(-a) as soon as the Member State responsible has been determined in accordance with	<i>This text is in square brackets in the Council text. Therefore, Council does not have a mandate yet to discuss this</i>

		<p>Regulation (EU) No XXX/XXX [Dublin Regulation] the [Member State conducting the procedures for determining the Member State responsible] shall update its data set recorded in conformity with Article 12 of this Regulation relating to the person concerned by adding the Member State responsible;]</p>	<p><i>text with the EP.</i></p>
<p>(a) when an applicant for international protection or another person as referred to in ⇒ Article 21(1) ⇐ ⇒ (b), (c), ⇐ (d) ⇒ or (e) ⇐ of Regulation (EU) No [...] 604/2013 arrives in the Member State responsible following a transfer pursuant to a decision acceding to a take back request ⇒ notification ⇐ as referred to in Article ⇒ 26 ⇐ thereof, the Member State responsible shall update its data set recorded in conformity with Article 11 12 of this Regulation relating to the person concerned by adding his or her date of arrival;</p>		<p>(a) when an applicant for international protection or another person as referred to in Article 20 [...] (1) (b), (c), (d) or (e) of Regulation (EU) No XXX/XXX [Dublin Regulation] [...] arrives in the Member State responsible following a transfer pursuant to a take back notification as referred to in Article 26 thereof, the Member State responsible shall update its data set recorded in conformity with Article 12 of this Regulation relating to the person concerned by adding his or her date of arrival;</p>	<p>(a) when an applicant for international protection or another person as referred to in Article 20 (1) (b), (c), (d) or (e) of Regulation (EU) No XXX/XXX [Dublin Regulation] arrives in the Member State responsible following a transfer pursuant to a take back notification as referred to in Article 26 thereof, the Member State responsible shall update its data set recorded in conformity with Article 12 of this Regulation relating to the person concerned by adding his or her date of arrival;</p>
<p>(b) when an applicant for international protection arrives in the Member State responsible following a transfer pursuant to a</p>		<p>(b) when an applicant for international protection arrives in the Member State responsible following a transfer pursuant to a</p>	<p>(b) when an applicant for international protection arrives in the Member State responsible following a transfer pursuant to a decision</p>

decision acceding to a take charge request according to Article ⇨ 24 ⇩ of Regulation (EU) No [...] 604/2013, the Member State responsible shall send a data set recorded in conformity with Article 11 12 of this Regulation relating to the person concerned and shall include his or her date of arrival;		decision acceding to a take charge request according to Article 24 of Regulation (EU) No XXX/XXX [Dublin Regulation] [...], the Member State responsible shall send a data set recorded in conformity with Article 12 of this Regulation relating to the person concerned and shall include his or her date of arrival;	acceding to a take charge request according to Article 24 of Regulation (EU) No XXX/XXX [Dublin Regulation], the Member State responsible shall send a data set recorded in conformity with Article 12 of this Regulation relating to the person concerned and shall include his or her date of arrival;
(c) when an applicant for international protection arrives in the Member State of allocation pursuant to Article 34 of Regulation (EU) No. [.../...], that Member State shall send a data set recorded in conformity with Article 12 of this Regulation relating to the person concerned and shall include his or her date of arrival and record that it is the Member State of allocation.		[(c) when an applicant for international protection arrives in the Member State of allocation pursuant to Article 36 [...] of Regulation (EU) No. XXX/XXX [Dublin Regulation] [...], that Member State shall send a data set recorded in conformity with Article 12 of this Regulation relating to the person concerned and shall include his or her date of arrival and record that it is the Member State of allocation.]	<i>This text is in square brackets in the Council text. Therefore, Council does not have a mandate yet to discuss this text with the EP.</i>
(c) as soon as the Member State of origin establishes that the person concerned whose data was recorded in Eurodac in accordance with Article 11 of this Regulation has left the territory of the Member States, it shall update its data set recorded in conformity with Article 11 of this Regulation			

relating to the person concerned by adding the date when that person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of Regulation (EU) No 604/2013;			
(d) as soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with Article 11 <u>12</u> of this Regulation has left the territory of the Member States in compliance with a return decision or removal order issued following the withdrawal or rejection of the application for international protection as provided for in Article 19(3) of Regulation (EU) No 604/2013 , it shall update its data set recorded in conformity with Article 11 <u>12</u> of this Regulation relating to the person concerned by adding the date of his or her removal or when he or she left the territory;			
(e) the Member State which becomes responsible in accordance with Article 19(1) of Regulation (EU) No 604/2013 shall update its data set recorded in conformity		(e) the Member State which becomes responsible in accordance with [Article 19(1) of Regulation (EU) No XXX/XXX [Dublin Regulation] [...]] shall update its data set recorded in conformity	(e) the Member State which becomes responsible in accordance with [Article 19(1) of Regulation (EU) No XXX/XXX [Dublin Regulation]] shall update its data set recorded in conformity with Article

with Article 11 12 of this Regulation relating to the applicant for international protection by adding the date when the decision to examine the application was taken.		with Article 12 of this Regulation relating to the applicant for international protection by adding the date when the decision to examine the application was taken.	12 of this Regulation relating to the applicant for international protection by adding the date when the decision to examine the application was taken.
<i>Article 11 12</i>		<i>Article 12</i>	
Recording of data		Recording of data	
Only the following data shall be recorded in the Central System:			
(a) fingerprint data;			
(b) a facial image;			
(c) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately;	Amendment 78 (c) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately;		<i>Confirmed by trilogue</i> (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);	Amendment 79 (d) nationality(ies) <i>or presumed and declared nationality(ies) or status as stateless person in accordance with Article 1(1) of the 1954 Convention relating to the Status</i>		<i>Confirmed by trilogue</i> (d) nationality(ies)

	<i>of Stateless Persons;</i>		
(e) place and date of birth;			
(b f) Member State of origin, place and date of the application for international protection; in the cases referred to in Article 10 11(b), the date of application shall be the one entered by the Member State who transferred the applicant;			
(e g) sex;			
(h) type and number of identity or travel document; three letter code of the issuing country and validity;		(h) where available , type and number of identity or travel document; three letter code of the issuing country and expiry date [...];	(h) where available , type and number of identity or travel document; three letter code of the issuing country and expiry date [...];
		(ha) 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;	<i>Confirmed by trilogue</i> (ha) 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;
(d i) reference number used by			


the Member State of origin;			
(j) unique application number of the application for international protection pursuant to Article 22(2) of Regulation (EU) No. [.../...];		[(j) unique application number of the application for international protection pursuant to Article 22(2) of Regulation (EU) No. XXX/XXX [Dublin Regulation] [...];]	<i>This text is in square brackets in the Council text. Therefore, Council does not have a mandate yet to discuss this text with the EP.</i>
		[(ja) the Member State responsible in accordance with Article 11(-a);]	<i>This text is in square brackets in the Council text. Therefore, Council does not have a mandate yet to discuss this text with the EP.</i>
(k) the Member State of allocation in accordance with Article 11(c);		[(k) the Member State of allocation in accordance with Article 11(c);]	<i>This text is in square brackets in the Council text. Therefore, Council does not have a mandate yet to discuss this text with the EP.</i>
(e) date on which the fingerprints ⇒ and/or facial image ⇐ were taken;		(l) date on which the biometric data [...] were taken;	(l) date on which the biometric data were taken;
(f m) date on which the data were transmitted to the Central System;			
(g n) operator user ID;			
(h o) where applicable in accordance with Article 10 11(a) or (b) , the date of the arrival of the person concerned after a successful transfer;			

<p>☒ (p) where applicable in accordance with Article 10 11(b), the date of the arrival of the person concerned after a successful transfer; ☒</p>			
<p>(q) where applicable in accordance with Article 11(c), the date of the arrival of the person concerned after a successful transfer;</p>		<p>[(q) where applicable in accordance with Article 11(c), the date of the arrival of the person concerned after a successful transfer;]</p>	<p><i>This text is in square brackets in the Council text. Therefore, Council does not have a mandate yet to discuss this text with the EP.</i></p>
<p>(i) where applicable in accordance with Article 10(c), the date when the person concerned left the territory of the Member States;</p>			
<p>(r) where applicable in accordance with Article 10 11(d), the date when the person concerned left or was removed from the territory of the Member States;</p>			
<p>(s) where applicable in accordance with Article 10 11(e), the date when the decision to examine the application was taken.</p>			
	<p>Amendment 80</p> <p><i>(sa) details of family members of minors, which are relevant for family tracing and reunification</i></p>		<p><i>Informal outcome of technical discussion - to be confirmed by trilogue</i></p> <p>Deletion</p>

	<i>such as their names, family link to the minor and, where available, their passport or identification card numbers.</i>		
--	---	--	--

PUBLIC

	Amendment 81 <p style="text-align: center;">CHAPTER II A: RESETTLED THIRD- COUNTRY NATIONALS OR STATELESS PERSONS</p>		<i>The Council does not have a mandate yet to discuss this text with the EP.</i>
	Amendment 82 <p style="text-align: center;"><i>Article 12a</i></p>		<i>The Council does not have a mandate yet to discuss this text with the EP.</i>
	<i>Collection and transmission of fingerprints and facial image data</i>		
	<i>1. Each Member State shall promptly take the fingerprints of all fingers and capture a facial image of every resettled third-country national or stateless person of at least six years of age, upon their arrival on its territory, and shall transmit the fingerprints and facial image, together with the other data referred to in Article 10 of Regulation (EU) .../..., to the Central System.</i>		
	<i>2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints,</i>		

	<i>the facial image or both of a resettled third-country national or stateless person on account of measures taken to ensure his or her health or the protection of public health, Member States shall take and send such fingerprints, facial image or both as soon as possible and no later than 48 hours after those health grounds no longer prevail.</i>		
--	---	---	--

	Amendment 83 <i>Article 12b</i>		<i>The Council does not have a mandate yet to discuss this text with the EP.</i>
	<i>Recording of data</i>		
	<i>Only the following data shall be recorded in the Central System:</i>		
	<i>(a) fingerprint data;</i>		
	<i>(b) a facial image;</i>		
	<i>(c) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately;</i>		
	<i>(d) nationality(ies);</i>		
	<i>(e) place and date of birth</i>		
	<i>(f) Member State of resettlement, place and date of the registration;</i>		
	<i>(g) sex;</i>		

	<i>(h) where applicable, the type and number of identity or travel document; three letter code of the issuing country and validity;</i>		
	<i>(i) reference number used by the Member State of origin;</i>		
	<i>(j) date on which the fingerprints and/or facial image were taken;</i>		
	<i>(k) date on which the data were transmitted to the Central System;</i>		
	<i>(l) operator user ID;</i>		
CHAPTER III		CHAPTER III	
<i>THIRD-COUNTRY NATIONALS OR STATELESS PERSONS APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER</i>		<i>THIRD-COUNTRY NATIONALS OR STATELESS PERSONS APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER</i>	
<i>Article 14 13</i>		<i>Article 13</i>	


Collection and transmission of fingerprint data ☒ and facial image data ☒		Collection and transmission of <u>biometric</u> [...] data	Collection and transmission of biometric data
<p>1. Each Member State shall promptly take the fingerprints of all fingers ⇒ and capture a facial image ⇐ of every third-country national or stateless person of at least 14 ⇒ six ⇐ years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn him or her back.</p>		<p>1. Each Member State shall promptly take the biometric data [...] of every third-country national or stateless person of at least six years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn him or her back.</p>	<p>1. Each Member State shall promptly take the biometric data of every third-country national or stateless person of at least six years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn him or her back.</p>
<p>2. The Member State concerned shall, as soon as possible and no later than 72 hours after the date of apprehension, transmit to the Central System the following data in relation to any third-country national or stateless person, as referred to in paragraph</p>			

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;	Amendment 84 (c) surname(s) and forename(s), name(s) at birth and previously used names;		<i>Confirmed by trilogue</i> (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);	Amendment 85 (d) nationality(ies) <i>or presumed and declared nationality(ies) or status as stateless person in accordance with Article 1(1) of the 1954 Convention relating to the Status of Stateless Persons;</i>		<i>Confirmed by trilogue</i> (d) nationality(ies)
(e) place and date of birth			
(bf) Member State of origin, place and date of the apprehension;			
(eg) sex;			
	Amendment 86 (ga) <i>details of family members of minors, which are relevant for</i>		<i>Informal outcome of technical discussion - to be confirmed by trilogue</i>

	<i>family tracing and reunification such as their names, family link to the minor and, where available, their passport or identification card numbers;</i>		Deletion
(h) type and number of identity or travel document; three letter code of the issuing country and validity;		(h) where available , type and number of identity or travel document; three letter code of the issuing country and expiry date [...];	(h) where available , type and number of identity or travel document; three letter code of the issuing country and expiry date [...];
		(ha) 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;	<i>Confirmed by trilogue</i> (ha) 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;
(ei) reference number used by the Member State of origin;			
	Amendment 87 (ia) <i>return decision taken, or removal order issued, by the Member State of origin;</i>		<i>Confirmed by trilogue</i> Deletion
(ei) date on which the fingerprints ⇒ and/or facial		(j) date on which the	(j) date on which the biometric

image ↵ were taken;		biometric data [...] were taken;	data were taken;
(k) date on which the data were transmitted to the Central System;			
(el) operator user ID ;			
(m) where applicable in accordance with paragraph 6, the date when the person concerned left or was removed from the territory of the Member States.			
3. By way of derogation from paragraph 2, the data specified in paragraph 2 relating to persons apprehended as described in paragraph 1 who remain physically on the territory of the Member States but are kept in custody, confinement or detention upon their apprehension for a period exceeding 72 hours shall be transmitted before their release from custody, confinement or detention.			
4. Non-compliance with the 72-hour time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the		4. Non-compliance with the 72-hour time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data [...] to the Central System. Where the condition of	4. Non-compliance with the 72-hour time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data to the Central System. Where the condition of the

<p>fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 25 26, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>		<p>the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>	<p>fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>
<p>5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints ⇨ and facial image ⇩ of the apprehended person on account of measures taken to ensure his or her health or the protection of public health, the Member State concerned shall take and send such fingerprints ⇨ and facial image ⇩ as soon as possible and no later than 48 hours after those health grounds no longer prevail.</p>		<p>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.</p>	<p>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.</p>
<p>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.</p>			

<p>6. As soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with paragraph (1) has left the territory of the Member States in compliance with a return decision or removal order, it shall update its data set recorded in conformity with paragraph (2) relating to the person concerned by adding the date of his or her removal or when he or she left the territory.</p>			
<p>7. Fingerprint data may also be taken and transmitted by members of the European Border [and Coast] Guard Teams when performing tasks and exercising powers in accordance with [Regulation on the European Border [and Coast] Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC].</p>	<p>Amendment 88</p> <p>7. Fingerprint Where requested by the Member State concerned, the biometric data may also be taken and transmitted by members of the European Border and Coast Guard Teams when performing tasks and exercising powers in accordance with [Regulation on the European Border [and Coast] Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC] Regulation (EU) 2016/1624 and by asylum support teams in accordance with [Regulation (EU)].</p>	<p>7. Where requested by the Member State concerned, the biometric [...] data may also be taken and transmitted by members of the European Border and Coast Guard Teams when performing tasks and exercising powers in accordance with Regulation (EU) 2016/1624 [...].</p>	<p><i>Confirmed by trilogue</i></p> <p><i>Where requested by the Member State concerned, the biometric</i> data may also be taken and transmitted <i>on behalf of that Member State</i> 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 <i>(EU) 2016/1624 and [Regulation (EU) No]</i>.</p>

Article 15			
Recording of data			
1. The data referred to in Article 14(2) shall be recorded in the Central System.			
Without prejudice to Article 8, data transmitted to the Central System pursuant to Article 14(2) shall be recorded solely for the purposes of comparison with data on applicants for international protection subsequently transmitted to the Central System and for the purposes laid down in Article 1(2).			
The Central System shall not compare data transmitted to it pursuant to Article 14(2) with any data previously recorded in the Central System, or with data subsequently transmitted to the Central System pursuant to Article 14(2).			
2. As regards the comparison of data on applicants for international protection subsequently transmitted to the Central System with the data referred to in			

paragraph 1, the procedures provided for in Article 9(3) and (5) and in Article 25(4) shall apply.			
Article 16			
Storage of data			
1. Each set of data relating to a third country national or stateless person as referred to in Article 14(1) shall be stored in the Central System for 18 months from the date on which his or her fingerprints were taken. Upon expiry of that period, the Central System shall automatically erase such data.			
2. The data relating to a third country national or stateless person as referred to in Article 14(1) shall be erased from the Central System in accordance with Article 28(3) as soon as the Member State of origin becomes aware of one of the following circumstances before the 18 month period referred to in paragraph 1 of this Article has expired:			
(a) the third country national or stateless person has been issued with a residence			

document;			
(b) the third country national or stateless person has left the territory of the Member States;			
(c) the third country national or stateless person has acquired the citizenship of any Member State.			
3. The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data for the reason specified in paragraph 2(a) or (b) of this Article by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).			
4. The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data for the reason specified in paragraph 2(c) of this Article by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or 14(1).			

CHAPTER IV		CHAPTER IV	
<i>THIRD-COUNTRY NATIONALS OR STATELESS PERSONS FOUND ILLEGALLY STAYING IN A MEMBER STATE</i>		<i>THIRD-COUNTRY NATIONALS OR STATELESS PERSONS FOUND ILLEGALLY STAYING IN A MEMBER STATE</i>	
<i>Article 17 14</i>		<i>Article 14</i>	
Comparison ☒ Collection and transmission ☒ of fingerprint ☒ and facial image ☒ data		Collection and transmission of <u>biometric</u> [...] data	Collection and transmission of biometric data
1. With a view to checking whether a third-country national or a stateless person found illegally staying within its territory has previously lodged an application for international protection in another Member State, a Member State may transmit to the Central System any fingerprint data relating to fingerprints which it may have taken of any such third-country national or stateless person of at least 14 years of age together with the reference number used by that Member State.			

As a general rule there are grounds for checking whether the third country national or stateless person has previously lodged an application for international protection in another Member State where:			
(a) the third country national or stateless person declares that he or she has lodged an application for international protection but without indicating the Member State in which he or she lodged the application;			
(b) the third country national or stateless person does not request international protection but objects to being returned to his or her country of origin by claiming that he or she would be in danger, or			
(c) the third country national or stateless person otherwise seeks to prevent his or her removal by refusing to cooperate in establishing his or her identity, in particular by showing no, or false, identity papers.			
2. Where Member States take part in the procedure referred to in			

paragraph 1, they shall transmit to the Central System the fingerprint data relating to all or at least the index fingers and, if those are missing, the prints of all the other fingers, of third-country nationals or stateless persons referred to in paragraph 1.			
1. Each Member State shall promptly take the fingerprints of all fingers and capture a facial image of every third-country national or stateless person of at least six years of age who is found illegally staying within its territory.		1. Each Member State shall promptly take the biometric data [...] of every third-country national or stateless person of at least six years of age who is found illegally staying within its territory.	1. Each Member State shall promptly take the biometric data of every third-country national or stateless person of at least six years of age who is found illegally staying within its territory.
2. The Member State concerned shall, as soon as possible and no later than 72-hours after the date of apprehension, transmit to the Central System the following data in relation to any third-country national or stateless person, as referred to in paragraph 1:			
(a) fingerprint data;			
(b) a facial image;			
(c) surname(s) and forename(s), name(s) at birth and previously used names and any			

aliases, which may be entered separately;			
(d) nationality(ies);	Amendment 89 <i>(d) nationality(ies) or presumed and declared nationality(ies) or status as stateless person in accordance with Article 1(1) of the 1954 Convention relating to the Status of Stateless Persons;</i>		<i>Confirmed by trilogue</i> (d) nationality(ies)
(e) place and date of birth			
(f) Member State of origin, place and date of the apprehension;			
(g) sex;			
	Amendment 90 <i>(ga) details of family members of minors, which are relevant for family tracing and reunification such as their names, family link to the minor and, where available, their passport or identification card numbers;</i>		<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> Deletion
(h) type and number of identity or travel document; three letter code of the issuing country		(h) where available , type and number of identity or travel document; three letter code of the issuing country and expiry date	(h) where available , type and number of identity or travel document; three letter code of the

and validity;		[...];	issuing country and expiry date [...];
		(ha) 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;	<i>Confirmed by trilogue</i> (ha) 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;
(i) reference number used by the Member State of origin;			
	Amendment 91 <i>(ia) return decision taken, or removal order issued, by the Member State of origin;</i>		<i>Confirmed by trilogue</i> Deletion
(j) date on which the fingerprints and/or facial image were taken;		(j) date on which the biometric data [...] were taken;	(j) date on which the biometric data were taken;
(k) date on which the data were transmitted to the Central System;			
(l) operator user ID;			
(m) where applicable in accordance with paragraph 6, the			

date when the person concerned left or was removed from the territory of the Member States			
	<p>Amendment 92</p> <p><i>2a. Member States may derogate from the provisions of paragraph 1 and 2 in respect of illegally staying third-country nationals who entered the Union by legally crossing the external border and have overstayed the authorised period of stay by a period of no more than 15 days.</i></p>		<p><i>Confirmed by trilogue</i></p> <p>Deletion + new recital 24a</p>
<p>3. The fingerprint data of a third-country national or a stateless person as referred to in paragraph 1 shall be transmitted to the Central System solely for the purpose of comparison ⇨ and compared ⇐ with the fingerprint data of applicants for international protection ⊗ persons fingerprinted for the purposes of Article 9 <u>10</u>(1), 14 <u>13</u>(1) and 17 <u>14</u>(1) <⊗ transmitted by other Member States and already recorded in the Central System.</p>		3. [...]	<p><i>Confirmed by trilogue</i></p> <p>Deletion</p>
The fingerprint data of such a third-country national or a stateless person shall not be recorded in the Central System.			

nor shall they be compared with the data transmitted to the Central System pursuant to Article 14(2).			
<p>4. Non-compliance with the 72-hour time-limit referred to in paragraph 3 of this Article shall not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>	<p>Amendment 93</p> <p>4. Non-compliance with the 72-hour time-limit referred to in paragraph 3 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data to the Central System. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>	<p>4. Non-compliance with the 72-hour time-limit referred to in paragraph 2 [...] of this Article shall not relieve Member States of the obligation to take and transmit the biometric data [...] to the Central System. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>	<p>4. Non-compliance with the 72-hour time-limit referred to in paragraph 2 of this Article shall not relieve Member States of the obligation to take and transmit the biometric data to the Central System. Where the condition of the fingertips does not allow the taking of fingerprints of a quality ensuring appropriate comparison under Article 26, the Member State of origin shall retake the fingerprints of persons apprehended as described in paragraph 1 of this Article, and resend them as soon as possible and no later than 48 hours after they have been successfully retaken.</p>
<p>5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints and facial image of the apprehended person on account of measures taken to ensure his or her health or the protection of public health, the Member State</p>		<p>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</p>	<p>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</p>

concerned shall take and send such fingerprints and facial image as soon as possible and no later than 48 hours after those health grounds no longer prevail.		and send such biometric data [...] as soon as possible and no later than 48 hours after those health grounds no longer prevail.	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 Article 13(1) of this Regulation has left the territory of the Member States in compliance with a return decision or removal order, it shall update its data set recorded in conformity with paragraph 2 of this Article relating to the person concerned by adding the date of his or her removal or when he or she left the territory.		6. As soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with paragraph 1 [...] has left the territory of the Member States in compliance with a return decision or removal order, it shall update its data set recorded in conformity with paragraph 2 [...] relating to the person concerned by adding the date of his or her removal or when he or she left the territory.	6. As soon as the Member State of origin ensures that the person concerned whose data was recorded in Eurodac in accordance with paragraph 1 has left the territory of the Member States in compliance with a return decision or removal order, it shall update its data set recorded in conformity with paragraph 2 relating to the person concerned by adding the date of his or her removal or when he or she left the territory.
4. Once the results of the comparison of fingerprint data have been transmitted to the Member State of origin, the record of the search shall be kept by the Central System only for the			

purposes of Article 28. Other than for those purposes, no other record of the search may be stored either by Member States or by the Central System.			
5. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for international protection transmitted by other Member States which have already been stored in the Central System, the procedures provided for in Article 9(3) and (5) and in Article 25(4) shall apply.			

<u>CHAPTER V</u>		CHAPTER V	
<p>⊠ PROCEDURE FOR COMPARISON OF DATA FOR APPLICANTS FOR INTERNATIONAL PROTECTION AND THIRD-COUNTRY NATIONALS APPREHENDED CROSSING THE BORDER IRREGULARLY OR ILLEGALLY STAYING IN THE TERRITORY OF A MEMBER STATE ⊠</p>	<p>Amendment 94</p> <p>PROCEDURE FOR COMPARISON OF DATA FOR APPLICANTS FOR INTERNATIONAL PROTECTION, <i>RESETTLED THIRD-COUNTRY NATIONALS AND STATELESS PERSONS</i> AND THIRD-COUNTRY NATIONALS APPREHENDED CROSSING THE BORDER IRREGULARLY OR ILLEGALLY STAYING IN THE TERRITORY OF A MEMBER STATE</p>	<p>PROCEDURE FOR COMPARISON OF DATA FOR APPLICANTS FOR INTERNATIONAL PROTECTION AND THIRD-COUNTRY NATIONALS AND STATELESS PERSONS APPREHENDED CROSSING THE BORDER IRREGULARLY OR ILLEGALLY STAYING IN THE TERRITORY OF A MEMBER STATE</p>	
<u>Article 15</u>		Article 15	
<p>⊠ Comparison of fingerprint and facial image data ⊠</p>		<p>Comparison of <u>biometric</u>[...]data</p>	<p>Comparison of biometric data</p>
<p>31. Fingerprint and facial image data within the meaning of Article 11(a) transmitted by any Member State, with the exception</p>	<p>Amendment 95</p> <p>1. Fingerprint <i>Biometric</i> and facial image data transmitted by</p>	<p>1. Biometric [...] data transmitted by any Member State, with the exception of those transmitted in accordance with</p>	<p><i>Text agreed with the exception of the reference to the Article on resettled persons' data</i></p>


<p>of those transmitted in accordance with Article 10 11(b) ⇒ and (c) ⇐ , shall be compared automatically with the fingerprint data transmitted by other Member States and already stored in the Central System ⊗ in accordance with Article 9 10(1), 14 13(1) and 17 14(1) ⊗ .</p>	<p>any Member State, with the exception of those transmitted in accordance with Article 11(b) and (c), shall be compared automatically with the fingerprint data transmitted by other Member States and already stored in the Central System in accordance with Article Articles 10(1), 12a, 13(1) and 14(1).</p>	<p>Article 11(b) and (c), shall be compared automatically with the biometric [...] data transmitted by other Member States and already stored in the Central System in accordance with Article 10(1), 13(1) and 14(1).</p>	<p>1. Biometric data transmitted by any Member State, with the exception of those transmitted in accordance with Article 11(b) and (c), shall be compared automatically with the biometric data transmitted by other Member States and already stored in the Central System in accordance with Article 10(1), [12a,] 13(1) and 14(1).</p>
<p>42. The Central System shall ensure, at the request of a Member State, that the comparison referred to in paragraph 3 1 ⊗ of this Article ⊗ covers the fingerprint ⇒ and facial image ⇐ data previously transmitted by that Member State, in addition to the ⊗ fingerprint ⊗ ⇒ and facial image ⇐ data from other Member States.</p>		<p>2. The Central System shall ensure, at the request of a Member State, that the comparison referred to in paragraph 1 of this Article covers the biometric [...] data previously transmitted by that Member State, in addition to the biometric [...] data from other Member States.</p>	<p>2. The Central System shall ensure, at the request of a Member State, that the comparison referred to in paragraph 1 of this Article covers the biometric data previously transmitted by that Member State, in addition to the biometric data from other Member States.</p>
<p>53. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin ⇒ following the procedures set out in Article 26(4) ⇐ . Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 11(a) to (k) ⇒ 12, 13(2) and 14(2) ⇐ along</p>	<p>Amendment 96</p> <p>3. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin following the procedures set out in Article 26(4). Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article</p>	<p>3. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin following the procedures set out in Article 26(4). Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 12, 13(2) and 14(2) along with, where appropriate, the mark referred to in</p>	<p><i>Text agreed with the exception of the reference to the Article on resettled persons' data</i></p> <p>3. The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin following the procedures set out in Article 26(4). Where there is a hit, it shall transmit for all data sets</p>


with, where appropriate, the mark referred to in Article 18 19(1) ⇒ and (4) ⇐ . ⇒ Where a negative hit result is received, the data referred to in Article 12, 13(2) and 14(2) shall not be transmitted. ⇐	Articles 12, 12b , 13(2) and 14(2) along with, where appropriate, the mark referred to in Article 19(1) and (4). Where a negative hit result is received, the data referred to in Article Articles 12, 12b , 13(2) and 14(2) shall not be transmitted.	Article 19(1) and (4). Where a negative [...] result is received, the data referred to in Article 12, 13(2) and 14(2) shall not be transmitted.	corresponding to the hit the data referred to in Article 12, [12b,] 13(2) and 14(2) along with, where appropriate, the mark referred to in Article 19(1) and (4). Where a negative result is received, the data referred to in Article 12, [12b,] 13(2) and 14(2) shall not be transmitted.
4. Where evidence of a hit is received by a Member State from Eurodac that can assist that Member State to carry out its obligations under Article 1(1)(a), that evidence shall take precedence over any other hit received.		4. Where [...] a hit is received by a Member State from Eurodac that can assist that Member State to carry out its obligations under Article 1(1)(a), that evidence shall take precedence over any other hit received.	4. Where a hit is received by a Member State from Eurodac that can assist that Member State to carry out its obligations under Article 1(1)(a), that evidence shall take precedence over any other hit received.
Article 16		Article 16	Article 16
Comparison of facial image data	Amendment 97 Comparison of facial image data <i>only</i>	Comparison of facial image data	<i>Confirmed by trilogue</i> Comparison of facial image data
(1) Where the condition of the fingertips does not allow for the taking of fingerprints of a quality ensuring appropriate comparison under Article 26 or where a person referred to in Article 10(1), 13(1) and 14(1) refuses to comply with the fingerprinting process, a Member State may carry out a comparison of facial image data as		(1) Where the condition of the fingertips does not allow for the taking of fingerprints of a quality ensuring appropriate comparison under Article 26 [...], a Member State shall [...] carry out a comparison of facial image data [...].	<i>Confirmed by trilogue</i> 1. Where the condition of the fingertips does not allow for the taking of fingerprints of a quality ensuring appropriate comparison under Article 26 or where no fingerprints are available for comparison , a Member State shall carry out a comparison of facial

a last resort.			image data.
(2) Facial image data and data relating to the sex of the data-subject may be compared automatically with the facial image data and personal data relating to the sex of the data-subject transmitted by other Member States and already stored in the Central System in accordance with Article 10(1), 13(1) and 14(1) with the exception of those transmitted in accordance with Article 11(b) and (c).	Amendment 98 (2) Facial image data and data relating to the sex of the data-subject may be compared automatically with the facial image data and personal data relating to the sex of the data-subject transmitted by other Member States and already stored in the Central System in accordance with Articles 10(1), 12a , 13(1) and 14(1) with the exception of those transmitted in accordance with Article 11(b) and (c).		<i>Text agreed with the exception of the reference to the Article on resettled persons' data</i> 2. Facial image data and data relating to the sex of the data-subject may be compared automatically with the facial image data and personal data relating to the sex of the data-subject transmitted by other Member States and already stored in the Central System in accordance with Articles 10(1), [12a,] 13(1) and 14(1) with the exception of those transmitted in accordance with Article 11(b) and (c).
(3) The Central System shall ensure, at the request of a Member State that the comparison referred to in paragraph 1 of this Article covers the facial image data previously transmitted by that Member State, in addition to the facial image data from other Member States.			
(4) The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin following the procedures set out in Article 26(4). Where	Amendment 99 (4) The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State	(4) The Central System shall automatically transmit the hit or the negative result of the comparison to the Member State of origin following the procedures set out in Article 26(5) [...]. Where	<i>Text agreed with the exception of the reference to the Article on resettled persons' data</i> 4. The Central System shall automatically transmit the hit or the

there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 12, 13(2) and 14(2) along with, where appropriate, the mark referred to in Article 17(1) and (4). Where a negative hit result is received, the data referred to in Article 12, 13(2) and 14(2) shall not be transmitted.	of origin following the procedures set out in Article 26(4). Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article Articles 12, 12b , 13(2) and 14(2) along with, where appropriate, the mark referred to in Article 17(1) 19(1) and (4). Where a negative hit result is received, the data referred to in Article Articles 12, 12b , 13(2) and 14(2) shall not be transmitted.	there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Article 12, 13(2) and 14(2) along with, where appropriate, the mark referred to in Article 19 [...] (1) and (4). Where a negative [...] result is received, the data referred to in Article 12, 13(2) and 14(2) shall not be transmitted.	negative result of the comparison to the Member State of origin following the procedures set out in Article 26(5). Where there is a hit, it shall transmit for all data sets corresponding to the hit the data referred to in Articles 12, [12b] , 13(2) and 14(2) along with, where appropriate, the mark referred to in Article 19(1) and (4). Where a negative hit result is received, the data referred to in Articles 12, [12b] , 13(2) and 14(2) shall not be transmitted.
(5) Where evidence of a hit is received by a Member State from Eurodac that can assist that Member State to carry out its obligations under Article 1(1)(a), that evidence shall take precedence over any other hit received.		(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.	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 V VI		CHAPTER VI	
BENEFICIARIES OF INTERNATIONAL PROTECTION ☒ DATA STORAGE, ADVANCED DATA ERASURE AND MARKING OF DATA ☒		DATA STORAGE, ADVANCED DATA ERASURE AND MARKING OF DATA	
Article 12 17		Article 17	
Data storage		Data storage	
<p>1. ☒ For the purposes laid down in Article 10(1), ☒ Each set of data ☒ relating to an applicant for international protection ☒, as referred to in Article 11 12, shall be stored in the Central System for ten years from the date on which the fingerprints were taken.</p>	<p>Amendment 100</p> <p>1. For the purposes laid down in Article 10(1), each set of data relating to an applicant for international protection, as referred to in Article 12, shall be stored in the Central System for ten five years from the date on which the fingerprints were first taken.</p>	<p>1. For the purposes laid down in Article 10(1), each set of data relating to an applicant for international protection, as referred to in Article 12, shall be stored in the Central System for ten years from the date on which the biometric data [...] were taken.</p>	<p><i>Rapporteur's proposals</i></p> <p><u>Option 1</u></p> <p>1. For the purposes laid down in Article 10(1), each set of data relating to an applicant for international protection, as referred to in Article 12, shall be stored in the Central System for ten five years from the date on which the fingerprints were first taken.</p> <p><i>1a. Before the expiry of the five-year storage period referred to in paragraph 1 of this Article, the Member State that is responsible for the examination of the application</i></p>


		 <p><i>for international protection in accordance with Regulation (EU) XXX/XXX [the Dublin Regulation] shall assess the need for continued storage of its set of data relating to an applicant for international protection, for the same purposes laid down in Article 10(1), and decide, on the basis of that review, to extend the storage period for another period of up to five years. The reasons for the continued storage shall be justified and recorded. If no decision is taken on the continued storage of the data set by the Member State responsible in accordance with Regulation (EU) XXX/XXX [the Dublin Regulation], that data set shall be automatically erased following the five-year period referred to in paragraph 1 of this Article.</i></p> <p>Relevant recital (new):</p> <p><i>The Member State that is responsible for the examination of the application for international protection in accordance with Regulation (EU) XXX/XXX [Dublin Regulation] should assess the need for continued storage of its data set relating to a an applicant for international protection for a period longer than five years due, in</i></p>
--	--	--

			<p><i>particular, to the fact that an applicant might leave the territory of the Member State responsible during the examination of the application for international protection or after a decision on the application is taken, which would necessitate the continued storage of its data set for the purposes of a take back procedure under Regulation (EU) XXX/XXX [the Dublin Regulation]. Where considering the need of the continued storage, the Member State should in particular take into account whether the applicant did conduct secondary movements and their frequency, as well as whether there are serious indications of a risk that the applicant will leave the territory of the responsible Member State before a decision on his application is taken or during the asylum procedure. A non-compliance of the applicant with the obligations related to making of the application and to cooperation with the competent authorities during the asylum procedure might be also taken into account for the consideration of the need of the continued storage.</i></p>
--	--	---	--


			<p><u>Option 2</u></p> <p><i>1a. By derogation from paragraph 1, the data set of the Member State responsible for the examination of the application for international protection of the applicant, in accordance with the Dublin Regulation, shall be stored in the Central System for ten years from the date on which the biometric data was taken.</i></p>
	<p>Amendment 101</p> <p><i>1a. For the purposes laid down in Article 12a, each set of data relating to a resettled third-country national or stateless person shall be kept in the Central System for five years from the date on which the fingerprints were taken.</i></p>		<p><i>The Council does not have a mandate yet to discuss this text with the EP.</i></p>
<p>2. For the purposes laid down in Article 13(1), each set of data relating to a third-country national or stateless person as referred to in Article 13(2) shall be stored in the Central System for five years from the date on which his or her fingerprints were taken.</p>	<p>Amendment 102</p> <p>2. For the purposes laid down in Article 13(1), each set of data relating to a third-country national or stateless person as referred to in Article 13(2) shall be stored in the Central System for <i>a period limited to the duration of a measure taken upon the third-</i></p>	<p>2. For the purposes laid down in Article 13(1), each set of data relating to a third-country national or stateless person as referred to in Article 13(2) shall be stored in the Central System for five years from the date on which his or her biometric data [...] were taken.</p>	<p><i>Confirmed by trilogue</i></p> <p>2. For the purposes laid down in Article 13(1), each set of data relating to a third-country national or stateless person as referred to in Article 13(2) shall be stored in the Central System for five years from the date on which his or her biometric data [...] were taken.</p>


	<i>country national or stateless person which shall not be more than</i> five years from the date on which his or her fingerprints were <i>first</i> taken.		
3. For the purposes laid down in Article 14(1), each set of data relating to a third-country national or stateless person as referred to in Article 14(2) shall be stored in the Central System for five years from the date on which his or her fingerprints were taken.	Amendment 103 3. For the purposes laid down in Article 14(1), each set of data relating to a third-country national or stateless person as referred to in Article 14(2) shall be stored in the Central System for <i>a period limited to the duration of a measure taken upon the third-country national or stateless person which shall not be more than</i> five years from the date on which his or her fingerprints were <i>first</i> taken.	3. For the purposes laid down in Article 14(1), each set of data relating to a third-country national or stateless person as referred to in Article 14(2) shall be stored in the Central System for five years from the date on which his or her biometric data [...] were taken.	<i>Confirmed by trilogue</i> 2. For the purposes laid down in Article 14(1), each set of data relating to a third-country national or stateless person as referred to in Article 13(2) shall be stored in the Central System for five years from the date on which his or her biometric data [...] were taken.
24. Upon expiry of the period <input type="checkbox"/> data storage periods <input type="checkbox"/> referred to in paragraphs 1 <input type="checkbox"/> to 3 <input type="checkbox"/> of this Article <input type="checkbox"/> , the Central System shall automatically erase the data <input type="checkbox"/> of the data-subjects <input type="checkbox"/> from the Central System.			

<i>Article 13 18</i>		<i>Article 18</i>	
Advance <input checked="" type="checkbox"/> Advanced <input checked="" type="checkbox"/> data erasure		Advanced data erasure	
<p>1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article 1217(1) \Rightarrow , (2) or (3) \Leftarrow shall be erased from the Central System in accordance with Article 27 28(4) as soon as the Member State of origin becomes aware that the person concerned has acquired such citizenship.</p>	<p>Amendment 104</p> <p>1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article 17(1) , (2) or (3) shall be erased from the Central System in accordance with Article 28(4)—as soon as. The Member State of origin becomes aware that <i>shall be informed immediately if</i> the person concerned has acquired such citizenship <i>in order to erase the data.</i></p>		<p><i>Confirmed by trilogue</i></p> <p><i>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 17(1), (2) or (3) shall be erased from the Central System without delay by that Member State in accordance with Article 28(4).</i></p> <p><i>Data relating to a person who has acquired the citizenship of another Member State before the expiry of the period referred to in Article 17(1), (2) or (3) shall be erased from the Central System by the Member State of origin, in accordance with Article 28(4), as soon as it becomes aware of the fact that the person concerned has acquired such citizenship.</i></p>
<p>2. The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data in accordance with</p>	<p>Amendment 105</p> <p>2. The Central System shall, as soon as possible and no later than after 72 hours, inform all</p>		<p><i>Text agreed with the exception of the reference to the Article on resettled persons' data</i></p> <p>2. The Central System shall, as</p>

<p>paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9 <u>10(1)</u>, or 14 <u>13(1)</u> \Rightarrow or 14(1) \Leftarrow .</p>	<p>Member States of origin of the erasure of data in accordance with paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article Articles 10(1), 12a, 13(1) or 14(1).</p>		<p>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 10(1), [12a], 13(1) or 14(1).</p>
<p><i>Article 18 <u>19</u></i></p>		<p><i>Article 19</i></p>	
<p>Marking of data</p>		<p>Marking of data</p>	
<p>1. For the purposes laid down in Article 1(1)(a), the Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded in the Central System pursuant to Article 11 <u>12</u> shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by \boxtimes eu-LISA \boxtimes the Agency. That mark shall be stored in the Central System in accordance with Article 12 <u>17(1)</u> for the purpose of transmission under Article 9(5) \Rightarrow 15 \Leftarrow . The Central System</p>	<p>Amendment 106</p> <p>1. For the purposes laid down in Article 1(1)(a), the Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded in the Central System pursuant to Article 12 shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by eu-LISA . That mark shall be stored in the Central System in accordance with Article 17(1) for the purpose of transmission under</p>	<p>1. For the purposes laid down in Article 1(1)(a), the Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded in the Central System pursuant to Article 12 shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by eu-LISA. That mark shall be stored in the Central System in accordance with Article 17(1) for the purpose of transmission under Article 15 and 16. The Central System shall, as soon as possible</p>	<p>1. For the purposes laid down in Article 1(1)(a), the Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded in the Central System pursuant to Article 12 shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by eu-LISA. That mark shall be stored in the Central System in accordance with Article 17(1) for the purpose of transmission under Article 15 and 16. The Central System shall, as soon as possible and no later than 72 hours, inform all Member States of origin of</p>

shall ⇒ , as soon as possible and no later than 72 hours, ⇨ inform all Member States of origin of the marking of data by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9 <u>10(1)</u> , or 14 <u>13(1)</u> ⇨ or 14(1) ⇨ . Those Member States of origin shall also mark the corresponding data sets.	Article 15 Articles 15 and 16. The Central System shall, as soon as possible and no later than 72 hours, inform all Member States of origin of the marking of data by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 10(1), 13(1) or 14(1). Those Member States of origin shall also mark the corresponding data sets.	and no later than 72 hours, inform all Member States of origin of the marking of data by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 10(1), 13(1) or 14(1). Those Member States of origin shall also mark the corresponding data sets.	the marking of data by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 10(1), 13(1) or 14(1). Those Member States of origin shall also mark the corresponding data sets.
2. The data of beneficiaries of international protection stored in the Central System and marked pursuant to paragraph 1 of this Article shall be made available for comparison for the purposes laid down in Article 1(2)(1)(c) <u>1(1)(c)</u> for a period of three years after the date on which the data subject was granted international protection.	Amendment 107 The data of beneficiaries of international protection stored in the Central System and marked pursuant to paragraph 1 of this Article shall be made available for comparison for the purposes laid down in Article 1(1)(c) for a period of three years after the date on which the data subject was granted international protection until such data are automatically erased from the Central System in accordance with Article 17(4).	2. The data of beneficiaries of international protection stored in the Central System and marked pursuant to paragraph 1 of this Article shall be made available for comparison for the purposes laid down in Article 1(1)(c) until such data is automatically erased from the Central System in accordance with Article 17(4) [...].	2. The data of beneficiaries of international protection stored in the Central System and marked pursuant to paragraph 1 of this Article shall be made available for comparison for the purposes laid down in Article 1(1)(c) until such data is automatically erased from the Central System in accordance with Article 17(4).
Where there is a hit, the Central System shall transmit the data referred to in Article 11 <u>12(a)</u> to (a) ⇨ (b) to (s) ⇨ for all the data sets corresponding to the hit. The		[...]	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> Deletion

<p>Central System shall not transmit the mark referred to in paragraph 1 of this Article. Upon the expiry of the period of three years, the Central System shall automatically block such data from being transmitted in the event of a request for comparison for the purposes laid down in Article 1(2) (1)(c), whilst leaving those data available for comparison for the purposes laid down in Article 1(1)(a) until the point of their erasure. Blocked data shall not be transmitted, and the Central System shall return a negative result to the requesting Member State in the event of a hit.</p>			
<p>3. The Member State of origin shall unmark or unblock data concerning a third-country national or stateless person whose data were previously marked or blocked in accordance with paragraphs 1 or 2 of this Article if his or her status is revoked or ended or the renewal of his or her status is refused under [Articles 14 or 19 of Directive 2011/95/EU].</p>		<p>3. The Member State of origin shall unmark [...] data concerning a third-country national or stateless person whose data were previously marked [...] in accordance with paragraphs 1 or 2 of this Article if his or her status is revoked or ended or the renewal of his or her status is refused under [Articles 14 or 19 of Directive 2011/95/EU].</p>	<p><i>Informal outcome of technical discussion - to be confirmed by trilogue</i></p> <p>3. The Member State of origin shall unmark data concerning a third-country national or stateless person whose data were previously marked in accordance with paragraphs 1 or 2 of this Article if his or her status is revoked or ended or the renewal of his or her status is refused under [Articles 14 or 19 of Directive 2011/95/EU].</p>

<p>4. For the purposes laid down in Article 1(1)(b), the Member State of origin which granted a residence document to an illegally staying third-country national or stateless person whose data were previously recorded in the Central System pursuant to Article 13(2) and 14(2) shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by eu-LISA. That mark shall be stored in the Central System in accordance with Article 17(2) and (3) for the purpose of transmission under Article 15 and 16. The Central System shall, as soon as possible and no later than 72-hours, inform all Member States of origin of the marking of data by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Articles 13(1) or 14(1). Those Member States of origin shall also mark the corresponding data sets.</p>			
<p>5. The data of illegally staying third-country nationals or stateless persons stored in the Central System and marked</p>			

pursuant to paragraph 4 of this Article shall be made available for comparison for the purposes laid down in Article 1(1)(c) until such data is automatically erased from the Central System in accordance with Article 17(4).			
CHAPTER VI VII		CHAPTER VII	
<i>PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES</i>		PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES	
<i>Article 19 20</i>		<i>Article 20</i>	
Procedure for comparison of fingerprint data with Eurodac data	Amendment 108 Procedure for comparison of fingerprint biometric or alphanumeric data with Eurodac data	Procedure for comparison of <u>biometric or alphanumeric</u> [...]data with Eurodac data	Procedure for comparison of <i>biometric or alphanumeric</i> data with Eurodac data
1. For the purposes laid down in Article 1(2)(1)(c), the designated authorities referred to in Articles 5 6(1) and 7 8(2) may submit a reasoned electronic	Amendment 109 1. For the purposes laid down in Article 1(1)(c), the designated authorities referred to in Articles	1. For the purposes laid down in Article 1(1)(c), the designated authorities referred to in Articles 6(1) and 8(2) may submit a reasoned electronic request as	<i>Confirmed by trilogue</i> 1. For the purposes laid down in Article 1(1)(c), the designated authorities referred to in Articles 6(1)

<p>request as provided for in Article 20 21(1) together with the reference number used by them, to the verifying authority for the transmission for comparison of fingerprint ⇒ and facial image ⇐ data to the Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether all the conditions for requesting a comparison referred to in Articles 20 21 or 21 22, as appropriate, are fulfilled.</p>	<p>6(1) and 8(2) may submit a reasoned electronic request as provided for in Article 21(1) together with the reference number used by them, to the verifying authority for the transmission for comparison of fingerprint and facial image biometric or alphanumeric data to the Central System, via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether all the conditions for requesting a comparison referred to in Articles 21 or 22, as appropriate, are fulfilled.</p>	<p>provided for in Article 21(1) together with the reference number used by them, to the verifying authority for the transmission for comparison of biometric data or alphanumeric [...] data to the Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether all the conditions for requesting a comparison referred to in Articles 21 or 22, as appropriate, are fulfilled.</p>	<p>[and 8(I)] may submit a reasoned electronic request as provided for in Article 21(1) and in Article 22(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 the Central System 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 21 or 22, as appropriate, are fulfilled.</p>
<p>2. Where all the conditions for requesting a comparison referred to in Articles 20 21 or 21 22 are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the Central System in accordance with Articles 9(3) and (5) ⇒ 15 and 16 ⇐ for the purpose of comparison with the ⊗ fingerprint ⊗ ⇒ and facial image ⇐ data transmitted to the Central System pursuant to Articles 9 10(1), and 14 13(2) ⇒ (1) and 14(1) ⇐ .</p>	<p>Amendment 110</p> <p>2. Where all the conditions for requesting a comparison referred to in Articles 21 or 22 are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the Central System in accordance with Articles 15 and 16 for the purpose of comparison with the fingerprint and facial image biometric or alphanumeric data transmitted to the Central System pursuant to Articles 10(1), 12a, 13 (1) and</p>	<p>2. Where all the conditions for requesting a comparison referred to in Articles 21 or 22 are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the Central System in accordance with Articles 15 and 16 for the purpose of comparison with the biometric or alphanumeric [...] data transmitted to the Central System pursuant to Articles 10(1), 13 (1) and 14(1).</p>	<p><i>Confirmed by trilogue (pending agreement on reference to the Article on resettled persons' data)</i></p> <p>2. Where all the conditions for requesting a comparison referred to in Articles 21 or 22 are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point or Europol Access Point which will process it to the Central System in accordance with Articles 15 and 16 for the purpose of comparison with the biometric or alphanumeric data transmitted to the Central System</p>

	14(1).		pursuant to Articles 10(1), [12 a] 13 (1) and 14(1).
	<p>Amendment 111</p> <p><i>2a. For the purposes laid down in Article 1(1)(c), Europol's designated authority may submit a reasoned electronic request as provided for in Article 22(1) for the comparison of biometric data or alphanumeric data to the Europol access point referred to in Article 8(2). Upon receipt of such a request, the Europol access point shall verify whether all the conditions for requesting a comparison referred to in Article 22 are fulfilled. Where all the conditions referred to in Article 22 are fulfilled, the duly authorised staff of the Europol access point shall process the request. The Eurodac data requested shall be transmitted to the operating unit referred to in Article 8(1) in such a way as to ensure the security of the data.</i></p>		<p><i>Confirmed by trilogue</i></p> <p>Deletion (AM 111 is now covered in Art. 8(1) and (2).</p>
3. A comparison of a facial image with other facial image data in the Central System pursuant to Article 1(1)(c) may be carried out in accordance with Article 16(1),			<p><i>Confirmed by trilogue</i></p> <p>3. A comparison of a facial image with other facial image data in the Central System pursuant to Article 1(1)(c) may be carried out in</p>

if such data is available at the time the reasoned electronic request is made pursuant to Article 21(1).			accordance with Article 16(1), if such data is available at the time the reasoned electronic request is made pursuant to Article 21(1) or Article 22(1) .
<u>34.</u> In exceptional cases of urgency where there is a need to prevent an imminent danger associated with a terrorist offence or other serious criminal offence, the verifying authority may transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions for requesting a comparison referred to in Article 20 21 or Article 21 22 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.	Amendment 112 4. In exceptional cases of urgency where there is a need to prevent an imminent danger associated with a terrorist offence or other serious criminal offence, the verifying authority may transmit the fingerprint biometric or alphanumeric data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions for requesting a comparison referred to in Article 21 or Article 22 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.	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 for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions for requesting a comparison referred to in Article 21 or Article 22 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.	<i>Confirmed by trilogue</i> 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 21 or Article 22 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.
<u>45.</u> 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.			
<i>Article 20 21</i>		<i>Article 21</i>	
Conditions for access to Eurodac by designated authorities		Conditions for access to Eurodac by designated authorities	
1. For the purposes laid down in Article 1(2)(1)(c), designated authorities may submit a reasoned electronic request for the comparison of fingerprint data with the data stored in the Central System within the scope of their powers only if comparisons with the following databases did not lead to the establishment of the identity of the data subject:	Amendment 113 1. For the purposes laid down in Article 1(1)(c), designated authorities may submit a reasoned electronic request for the comparison of fingerprint biometric or alphanumeric data with the data stored in the Central System within the scope of their powers only if comparisons with the following databases did not lead to the establishment of the identity of the data subject prior check has been conducted in:	1. For the purposes laid down in Article 1(1)(c), designated authorities may submit a reasoned electronic request for the comparison of biometric or alphanumeric [...] data with the data stored in the Central System within the scope of their powers only if a prior check has been conducted in [...] :	1. For the purposes laid down in Article 1(1)(c), designated authorities may submit a reasoned electronic request for the comparison of biometric or alphanumeric data with the data stored in the Central System within the scope of their powers only if a prior check has been conducted in:
– national fingerprint databases;		– national [...]databases; and	<i>Confirmed by trilogue</i> - national [...] databases; and
– the automated fingerprinting identification systems of all other Member States under	Amendment 114 - the automated	– the automated fingerprinting identification systems of all other Member States under	<i>Confirmed by trilogue</i> - the automated fingerprinting


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	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	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; [...]	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;
– the Visa Information System provided that the conditions for such a comparison laid down in Decision 2008/633/JHA are met;		– [...]	<i>Confirmed by trilogue</i> Deletion + new text in Article 21(1) last subparagraph
and where the following cumulative conditions are met:			
(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, which means that there is an overriding public security concern which makes the searching of the database			





proportionate;			
(b) the comparison is necessary in a specific case (i.e. systematic comparisons shall not be carried out); and		(b) the comparison is necessary in a specific case or to specific persons [...]; and	<p><i>Confirmed by trilogue</i></p> <p>(b) the comparison is necessary in a specific case including specific persons [...]; and</p>
(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.			
			<p><i>Confirmed by trilogue</i></p> <p><i>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</i></p>

			<i>first subparagraph at the same time they submit a request for comparison with the data stored in the Visa Information System.</i>
2. Requests for comparison with Eurodac data shall be limited to searching with fingerprint \Rightarrow or facial image \Leftarrow data.	Amendment 115 2. Requests for comparison with Eurodac data shall be limited to searching with fingerprint or facial image biometric or alphanumeric data.	2. Requests for comparison with Eurodac data for the purposes of Article 1(1)(c) shall be carried out [...]with biometric or alphanumeric [...] data.	<i>Confirmed by trilogue</i> 2. Requests for comparison with Eurodac data for the purposes of Article 1(1)(c) shall be carried out with biometric or alphanumeric data.
<i>Article 21 22</i>		<i>Article 22</i>	
Conditions for access to Eurodac by Europol		Conditions for access to Eurodac by Europol	
1. For the purposes laid down in Article 1(2)(1)(c), Europol's designated authority may submit a reasoned electronic request for the comparison of fingerprint data with the data stored in the Central System within the limits of Europol's mandate and where necessary for the performance of Europol's tasks only if comparisons with fingerprint data stored in any information processing systems that are technically and legally accessible by Europol did not lead to the establishment of the identity of the		1. For the purposes laid down in Article 1(1)(c), Europol's designated authority may submit a reasoned electronic request for the comparison of biometric or alphanumeric [...] data with the data stored in the Central System within the limits of Europol's mandate and where necessary for the performance of Europol's tasks only if comparisons with biometric or alphanumeric [...] data stored in any information processing systems that are technically and legally accessible by Europol did not lead to the	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> 1. For the purposes laid down in Article 1(1)(c), Europol's designated authority may submit a reasoned electronic request for the comparison of biometric or alphanumeric [...] data with the data stored in the Central System within the limits of Europol's mandate and where necessary for the performance of Europol's tasks only if comparisons with biometric or alphanumeric [...] data stored in any information

data subject and where the following cumulative conditions are met:		establishment of the identity of the data subject and where the following cumulative conditions are met:	processing systems that are technically and legally accessible by Europol did not lead to the establishment of the identity of the data subject and where the following cumulative conditions are met:
(a) the comparison is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate, which means that there is an overriding public security concern which makes the searching of the database proportionate;			
(b) the comparison is necessary in a specific case (i.e. systematic comparisons shall not be carried out); and		(b) the comparison is necessary in a specific case or to specific persons [...]; and	<i>Confirmed by trilogue</i> (b) the comparison is necessary in a specific case <u>including</u> specific persons ; and
(c) there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. Such reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a			

terrorist offence or other serious criminal offence falls in a category covered by this Regulation.			
2. Requests for comparison with Eurodac data shall be limited to comparisons of fingerprint ⇒ and facial image ⇐ data.	Amendment 116 2. Requests for comparison with Eurodac data shall be limited to comparisons of fingerprint and facial image biometric or alphanumeric data	2. Requests for comparison with Eurodac data for the purposes of Article 1(1)(c) shall be carried out with [...] biometric or alphanumeric [...] data.	2. Requests for comparison with Eurodac data for the purposes of Article 1(1)(c) shall be carried out with biometric or alphanumeric data.
3. Processing of information obtained by Europol from comparison with Eurodac data shall be subject to the authorisation of the Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.			
	Amendment 117 <i>3a. Europol may request further information from the Member State concerned in accordance with Regulation (EU) 2016/794.</i>		<i>Confirmed by trilogue</i> Deletion
	Amendment 118 <i>3b. The processing of personal data as a result of the access referred to in paragraph 1 shall be carried out in compliance</i>		<i>Informal outcome of technical discussions - to be confirmed by trilogue</i> Deletion

	<p><i>with the data protection safeguards provided for in Regulation (EU) 2016/794. Europol shall keep records of all searches and access to the Central System and shall make that documentation available, upon request, to the Data Protection Officer appointed pursuant to Regulation (EU) 2016/794 and to the European Data Protection Supervisor for the purpose of verifying the lawfulness of the data processing.</i></p>		
	<p>Amendment 119</p> <p><i>3 c. Personal data obtained as a result of a search in the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union unless such a transfer is strictly necessary and proportionate in cases falling within Europol's mandate. Any such transfer shall be carried out in accordance with Chapter V of Regulation (EU) 2016/794 and subject to the consent of the Member State of origin.</i></p>		<p><i>Under discussion</i></p>


<i>Article 22 23</i>		<i>Article 23</i>	
Communication between the designated authorities, the verifying authorities and the National Access Points		Communication between the designated authorities, the verifying authorities and the National Access Points	<p><i>Confirmed by trilogue</i></p> <p>Communication between the designated authorities, the verifying authorities, the National Access Points and the Europol Access Point</p>
<p>1. Without prejudice to Article 26 27, all communication between the designated authorities, the verifying authorities and the National Access Points shall be secure and take place electronically.</p>			<p><i>Confirmed by trilogue</i></p> <p>1. Without prejudice to Article 27, 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.</p>
<p>2. For the purposes laid down in Article 1(2)(1)(c), fingerprints shall be digitally processed by the Member States and transmitted in the data format referred to  as set out  in  the agreed Interface Control Document  Annex I, in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.</p>		<p>2. For the purposes laid down in Article 1(1)(c), searches with biometric or alphanumeric data [...] shall be digitally processed by the Member States and transmitted in the data format as set out in the agreed Interface Control Document, in order to ensure that the comparison can be carried out with other data stored in the Central System.</p>	<p><i>Confirmed by trilogue</i></p> <p>2. For the purposes laid down in Article 1(1)(c), 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 the Central System.</p>

CHAPTER VII <u>VIII</u>		CHAPTER VIII	
<i>DATA PROCESSING, DATA PROTECTION AND LIABILITY</i>		<i>DATA PROCESSING, DATA PROTECTION AND LIABILITY</i>	
<i>Article 23 24</i>		<i>Article 24</i>	
Responsibility for data processing		Responsibility for data processing	
1. The Member State of origin shall be responsible for ensuring that:			
(a) fingerprints ⇨ and facial images ⇨ are taken lawfully;		(a) biometric data and the other data referred to in Article 12, Article 13(2) and Article 14(2) [...]are taken lawfully;	<i>Confirmed by trilogue</i> (a) biometric data and the other data referred to in Article 12, Article 13(2) and Article 14(2) [...]are taken lawfully;
(b) fingerprint data and the other data referred to in Article 11 <u>12</u> , Article 14 <u>13</u> (2) and Article 17 <u>14</u> (2) are lawfully transmitted to the Central System;	Amendment 120 (b) fingerprint data and the other data referred to in Article 12, Article 12b , Article 13(2) and Article 14(2) are lawfully transmitted to the Central System;	(b) biometric [...] data and the other data referred to in Article 12, Article 13(2) and Article 14(2) are lawfully transmitted to the Central System;	<i>Text agreed with the exception of the reference to the Article on resettled persons' data</i> (b) biometric data and the other data referred to in Article 12, Article [12b] , Article 13(2) and Article 14(2) are lawfully transmitted to the Central System;

(c) data are accurate and up-to-date when they are transmitted to the Central System;			
(d) without prejudice to the responsibilities of the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> the Agency, data in the Central System are lawfully recorded, stored, corrected and erased;		(d) without prejudice to the responsibilities of eu-LISA, data in the Central System are lawfully recorded, stored, rectified [...] and erased;	<i>Confirmed by trilogue</i> (d) without prejudice to the responsibilities of eu-LISA, data in the Central System are lawfully recorded, stored, rectified and erased;
(e) the results of fingerprint <input checked="" type="checkbox"/> and facial image <input checked="" type="checkbox"/> data comparisons transmitted by the Central System are lawfully processed.		(e) the results of biometric [...] data comparisons transmitted by the Central System are lawfully processed.	<i>Confirmed by trilogue</i> (e) the results of biometric data comparisons transmitted by the Central System are lawfully processed.
2. In accordance with Article 34 <u>36</u> , the Member State of origin shall ensure the security of the data referred to in paragraph 1 before and during transmission to the Central System as well as the security of the data it receives from the Central System.			
3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article 25 <u>26</u> (4).			
4. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall ensure that the			<i>Confirmed by trilogue</i> 4. eu-LISA shall ensure that the

Central System is operated in accordance with the provisions of this Regulation. In particular, the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall:			Central System is operated, including where <i>operated for testing purposes</i> , in accordance with the provisions of this Regulation <i>and of relevant Union data protection rules</i> . In particular, eu-LISA shall:
(a) adopt measures ensuring that persons working with the Central System process the data recorded therein only in accordance with the purposes of Eurodac as laid down in Article 1;			<i>Confirmed by trilogue</i> (a) adopt measures ensuring that all persons, including contractors , working with the Central System process the data recorded therein only in accordance with the purposes of Eurodac as laid down in Article 1;
(b) take the necessary measures to ensure the security of the Central System in accordance with Article 34 <u>36</u> ;			
(c) ensure that only persons authorised to work with the Central System have access thereto, without prejudice to the competences of the European Data Protection Supervisor.			
The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> 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.			

<i>Article 24 25</i>		<i>Article 25</i>	
Transmission		Transmission	
<p>1. Fingerprints shall be digitally processed and transmitted in the data format referred to as set out in the agreed Interface Control Document Annex I. As far as necessary for the efficient operation of the Central System, the Agency eu-LISA shall establish the technical requirements for transmission of the data format by Member States to the Central System and vice versa. The Agency eu-LISA shall ensure that the fingerprint data and facial images transmitted by the Member States can be compared by the computerised fingerprint and facial recognition system.</p>		<p>1. Biometric data and other personal data [...] shall be digitally processed and transmitted in the data format as set out in the agreed Interface Control Document. As far as necessary for the efficient operation of the Central System, eu-LISA shall establish the technical requirements for transmission of the data format by Member States to the Central System and vice versa. eu-LISA shall ensure that the biometric [...] data transmitted by the Member States can be compared by the computerised fingerprint and facial recognition system.</p>	<p>1. Biometric data and other personal data shall be digitally processed and transmitted in the data format as set out in the agreed Interface Control Document. As far as necessary for the efficient operation of the Central System, eu-LISA shall establish the technical requirements for transmission of the data format by Member States to the Central System and vice versa. eu-LISA shall ensure that the biometric data transmitted by the Member States can be compared by the computerised fingerprint and facial recognition system.</p>
<p>2. Member States shall transmit the data referred to in Article 11 12, Article 14 13(2) and Article 17 14(2) electronically. The data referred to in Article 11 12, and Article 14 13(2) and Article 14(2) shall be automatically recorded in the</p>	<p>Amendment 121</p> <p>2. Member States shall transmit the data referred to in Article 12, Article 12b, Article 13(2) and Article 14(2) electronically. The data referred to in Article 12, Article 12b, Article</p>		<p><i>Text agreed with the exception of the references to the Article on resettled persons's data</i></p> <p>2. Member States shall transmit the data referred to in Article 12, Article [12b], Article 13(2) and Article 14(2) electronically. The data</p>

<p>Central System. As far as necessary for the efficient operation of the Central System, the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central System and vice versa.</p>	<p>13(2) and Article 14(2) shall be automatically recorded in the Central System. As far as necessary for the efficient operation of the Central System, eu-LISA shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central System and vice versa</p>		<p>referred to in Article 12, Article [12b], Article 13(2) and Article 14(2) shall be automatically recorded in the Central System. As far as necessary for the efficient operation of the Central System, eu-LISA shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central System and vice versa</p>
<p>3. The reference number referred to in Articles 11(d) 12(i), 14(2)(d) 13(2)(i), 17 14(1) <input checked="" type="checkbox"/> (2)(i) <input checked="" type="checkbox"/> and 19 20(1) shall make it possible to relate data unambiguously to one particular person and to the Member State which is transmitting the data. In addition, it shall make it possible to tell whether such data relate to a person referred to in Article 9 10(1), 14 13(1) or 17 14(1).</p>	<p>Amendment 122</p> <p>3. The reference number referred to in Articles 12(i), 12b(i), 13(2)(i), 14 (2)(i) and 20(1) shall make it possible to relate data unambiguously to one particular person and to the Member State which is transmitting the data. In addition, it shall make it possible to tell whether such data relate to a person referred to in Articles 10(1), 12a, 13(1) or 14(1).</p>		<p><i>Text agreed with the exception of the references to the Articles on resettled persons' data</i></p> <p>3. The reference number referred to in Articles 12(i), [12b(i)], 13(2)(i), 14 (2)(i) and 20(1) shall make it possible to relate data unambiguously to one particular person and to the Member State which is transmitting the data. In addition, it shall make it possible to tell whether such data relate to a person referred to in Articles 10(1), [12a,] 13(1) or 14(1).</p>
<p>4. The reference number shall begin with the identification letter or letters by which, in accordance with the norm referred to in Annex I, the Member State transmitting the data is identified. The identification letter or letters shall</p>	<p>Amendment 123</p> <p>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</p>		<p><i>Text agreed with the exception of the references to the Articles on resettled persons' data</i></p> <p>4. The reference number shall begin with the identification letter or letters by which the Member State transmitting the data is identified. The</p>

be followed by the identification of the category of person or request. "1" refers to data relating to persons referred to in Article 9 <u>10</u> (1), "2" to persons referred to in Article 14 <u>13</u> (1), "3" to persons referred to in Article 17 <u>14</u> (1), "4" to requests referred to in Article 20 <u>21</u> , "5" to requests referred to in Article 21 <u>22</u> and "9" to requests referred to in Article 29 <u>30</u> .	identification of the category of person or request. "1" refers to data relating to persons referred to in Article 10(1), "2" to persons referred to in Article 13(1), "3" to persons referred to in Article 14(1), "4" to requests referred to in Article 21, "5" to requests referred to in Article 22, "9" to requests referred to in Article 30, and "6" to requests referred to in Article 12a.		identification letter or letters shall be followed by the identification of the category of person or request. "1" refers to data relating to persons referred to in Article 10(1), "2" to persons referred to in Article 13(1), "3" to persons referred to in Article 14(1), "4" to requests referred to in Article 21, "5" to requests referred to in Article 22, "9" to requests referred to in Article 30, [and "6" to requests referred to in Article 12a].
5. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central System.			
6. The Central System shall confirm receipt of the transmitted data as soon as possible. To that end, the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.			
<i>Article 25 <u>26</u></i>		<i>Article 26</i>	
Carrying out comparisons and transmitting results		Carrying out comparisons and transmitting results	

<p>1. Member States shall ensure the transmission of fingerprint data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint ⇨ and facial ⇨ recognition system. As far as necessary to ensure that the results of the comparison by the Central System reach a very high level of accuracy, the Agency ⇨ eu-LISA ⇨ shall define the appropriate quality of transmitted fingerprint data. The Central System shall, as soon as possible, check the quality of the fingerprint ⇨ and facial image ⇨ data transmitted. If fingerprint ⇨ or facial image ⇨ data do not lend themselves to comparison using the computerised fingerprint ⇨ and facial ⇨ recognition system, the Central System shall inform the Member State concerned. That Member State shall then transmit fingerprint ⇨ or facial image ⇨ data of the appropriate quality using the same reference number as the previous set of fingerprint ⇨ or facial image ⇨ data.</p>		<p>1. Member States shall ensure the transmission of biometric [...] data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint and facial recognition system. As far as necessary to ensure that the results of the comparison by the Central System reach a very high level of accuracy, eu-LISA shall define the appropriate quality of transmitted biometric [...] data. The Central System shall, as soon as possible, check the quality of the biometric [...] data transmitted. If the biometric [...] data do not lend themselves to comparison using the computerised fingerprint and facial recognition system, the Central System shall inform the Member State concerned. That Member State shall then transmit biometric [...] data of the appropriate quality using the same reference number as the previous set of biometric [...] data.</p>	<p>1. Member States shall ensure the transmission of biometric data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint and facial recognition system. As far as necessary to ensure that the results of the comparison by the Central System reach a very high level of accuracy, eu-LISA shall define the appropriate quality of transmitted biometric data. The Central System shall, as soon as possible, check the quality of the biometric data transmitted. If the biometric data do not lend themselves to comparison using the computerised fingerprint and facial recognition system, the Central System shall inform the Member State concerned. That Member State shall then transmit biometric data of the appropriate quality using the same reference number as the previous set of biometric data.</p>
<p>2. The Central System shall carry out comparisons in the order</p>			

<p>of arrival of requests. Each request shall be dealt with within 24 hours. A Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where such time-limits cannot be respected owing to circumstances which are outside the Agency's ☒ eu-LISA's ☒ responsibility, the Central System shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as is necessary for the efficient operation of the Central System, the Agency ☒ eu-LISA ☒ shall establish criteria to ensure the priority handling of requests.</p>			
<p>3. As far as necessary for the efficient operation of the Central System, the Agency ☒ eu-LISA ☒ shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.</p>			
<p>4. The result of the comparison ☒ of fingerprint data carried out pursuant to Article 15 ☒ shall be immediately</p>	<p>Amendment 124</p> <p>4. The result of the comparison of <i>fingerprints and</i></p>	<p>4. The result of the comparison of fingerprint data carried out pursuant to Article 15 shall be immediately checked in</p>	<p><i>Confirmed by trilogue (some modifications were proposed and informally agreed at technical level on a suggestion by EP lawyer</i></p>

<p>checked in the receiving Member State by a fingerprint expert as defined in accordance with its national rules, specifically trained in the types of fingerprint comparisons provided for in this Regulation. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned, pursuant to Article 34 of Regulation (EU) No 604/2013.</p>	<p><i>facial image</i> carried out pursuant to Article 15 shall be immediately checked in the receiving Member State by a fingerprint <i>and facial identification</i> expert as defined in accordance with its national rules, specifically trained in the types of fingerprint <i>and facial image</i> comparisons provided for in this Regulation. For the purposes laid down in Article 1(1)(a), (aa) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.</p>	<p>the receiving Member State, where necessary by a fingerprint expert as defined in accordance with its national rules, specifically trained in the types of fingerprint comparisons provided for in this Regulation. Where the Central System returns a hit based on fingerprint and facial image data Member States may check and verify the facial image result if needed. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.</p>	<p><i>linguists)</i></p> <p>4. The result of the comparison of fingerprint data carried out pursuant to Article 15 shall be immediately checked in the receiving Member State, <u>Where necessary, by a fingerprint expert <i>in the receiving Member State</i>, as defined in accordance with its national rules, <i>and</i> specifically trained in the types of fingerprint comparisons provided for in this Regulation, <i>shall immediately check the result of the comparison of fingerprint data carried out pursuant to Article 15.</i></u></p> <p><u>Where, following a comparison of both fingerprint and facial image data with data recorded in the computerised central database, the Central System returns a fingerprint hit and a facial image <i>hit</i> data, Member States may check and verify the result of the comparison of the facial image data.</u></p> <p>For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.</p>
---	---	--	--


<p>5. The result of the comparison of facial image data carried out pursuant to Article 16 shall be immediately checked and verified in the receiving Member State. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.</p>	<p>Amendment 125</p> <p>The result of the comparison of facial image data carried out pursuant to Article 16 shall be immediately checked and verified in the receiving Member State, <i>where necessary by a specially trained expert and in accordance with its national rules</i>. For the purposes laid down in Article 1(1)(a), <i>(aa)</i> and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.</p>	<p>5. The result of the comparison of facial image data carried out pursuant to Article 15, 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. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.</p>	<p><i>Confirmed by trilogue</i></p> <p>5. The result of the comparison of facial image data carried out pursuant to Article 15, 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 <i>by an official trained in accordance with national practice</i>. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, final identification shall be made by the Member State of origin in cooperation with the other Member States concerned.</p>
<p>Information received from the Central System relating to other data found to be unreliable shall be erased as soon as the unreliability of the data is established.</p>			
<p><u>56.</u> Where final identification in accordance with paragraph 4 reveals that the result of the comparison received from the Central System does not correspond to the fingerprint ⇒ or facial image ⇐ data sent for comparison, Member States shall immediately erase the result of the</p>		<p>6. Where final identification in accordance with paragraph 4 and 5 reveals that the result of the comparison received from the Central System does not correspond to the biometric [...] data sent for comparison, Member States shall immediately erase the result of the comparison and</p>	<p><i>Confirmed by trilogue</i></p> <p>6. Where final identification in accordance with paragraph 4 and 5 reveals that the result of the comparison received from the Central System does not correspond to the biometric [...] data sent for comparison, Member States shall</p>

<p>comparison and communicate this fact as soon as possible and no later than after three working days to the Commission and to eu-LISA the Agency and inform them of the reference number of the Member State of origin and the reference number of the Member State that received the result .</p>		<p>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.</p>	<p>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</p>
<p><i>Article 26 27</i></p>		<p><i>Article 27</i></p>	
<p>Communication between Member States and the Central System</p>		<p>Communication between Member States and the Central System</p>	
<p>Data transmitted from the Member States to the Central System and vice versa shall use the Communication Infrastructure. As far as is necessary for the efficient operation of the Central System, the Agency eu-LISA shall establish the technical procedures necessary for the use of the Communication Infrastructure.</p>			
<p><i>Article 27 28</i></p>		<p><i>Article 28</i></p>	
<p>Access to, and correction or erasure of, data recorded in</p>		<p>Access to, and rectification [...] or erasure of, data recorded in</p>	<p>Access to, and rectification or erasure of, data recorded in</p>

Eurodac		Eurodac	Eurodac
1. The Member State of origin shall have access to data which it has transmitted and which are recorded in the Central System in accordance with this Regulation.			
No Member State may conduct searches of the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in Article 9(5) ⇒ 15 and 16 ⇐ .			
2. The authorities of Member States which, pursuant to paragraph 1 of this Article, have access to data recorded in the Central System shall be those designated by each Member State for the purposes laid down in Article 1(1)(a) and (b). That designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and the Agency ⇔ eu-LISA ⇔ a list of those units and any amendments thereto. The Agency ⇔ eu-LISA ⇔ shall publish the	Amendment 126 2. The authorities of Member States which, pursuant to paragraph 1 of this Article, have access to data recorded in the Central System shall be those designated by each Member State for the purposes laid down in Article 1(1)(a), (aa) and (b). That designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and eu-LISA a list of those units and any amendments thereto. eu-LISA shall publish the		<i>Text agreed with the exception of the reference to the Article on resettled persons' data</i> 2. The authorities of Member States which, pursuant to paragraph 1 of this Article, have access to data recorded in the Central System shall be those designated by each Member State for the purposes laid down in Article 1(1)(a), [(aa)] and (b). That designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and eu-LISA a list of those units and any amendments thereto. eu-LISA shall publish the

consolidated list in the <i>Official Journal of the European Union</i> . Where there are amendments thereto, the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall publish once a year an updated consolidated list online.	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.		consolidated list in the Official Journal of the European Union. Where there are amendments thereto, eu-LISA shall publish once a year an updated consolidated list online.
3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central System by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 12(2) or 16(1) .		3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central System by rectifying [...] or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article 18.	3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central System by rectifying or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article 18.
4. If a Member State or the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> has evidence to suggest that data recorded in the Central System are factually inaccurate, it shall <input checked="" type="checkbox"/> , without prejudice to the notification of a personal data breach pursuant to Article [33..] of Regulation (EU) No [.../2016], <input checked="" type="checkbox"/> advise the Member State of origin as soon as possible.		4. If a Member State or eu-LISA has evidence to suggest that data recorded in the Central System are factually inaccurate, it shall, without prejudice to the notification of a personal data breach pursuant to Article 33 of Regulation (EU) No 2016/679 [...], advise the Member State of origin as soon as possible.	4. If a Member State or eu-LISA has evidence to suggest that data recorded in the Central System are factually inaccurate, it shall, without prejudice to the notification of a personal data breach pursuant to Article 33 of Regulation (EU) No 2016/679 , advise the Member State of origin as soon as possible.
If a Member State has evidence to suggest that data were recorded in the Central System in breach of this Regulation, it shall advise			

<p>☒ eu-LISA ☒ the Agency, the Commission and the Member State of origin as soon as possible. The Member State of origin shall check the data concerned and, if necessary, amend or erase them without delay.</p>			
<p>5. The Agency ☒ eu-LISA ☒ shall not transfer or make available to the authorities of any third country data recorded in the Central System. This prohibition shall not apply to transfers of such data to third countries to which Regulation (EU) No [.../...] 604/2013 applies.</p>		<p>5. eu-LISA shall not transfer or make available to the authorities of any third country data recorded in the Central System. This prohibition shall not apply to transfers of such data to third countries to which Regulation (EU) No XXX/XXX [Dublin Regulation] [...] applies.</p>	<p><i>Confirmed by trilogue</i></p> <p>5. eu-LISA shall not transfer or make available to the authorities of any third country data recorded in the Central System. This prohibition shall not apply to transfers of such data to third countries to which Regulation (EU) No XXX/XXX [Dublin Regulation] applies.</p>
<p><i>Article 28 29</i></p>		<p><i>Article 29</i></p>	
<p>Keeping of records</p>		<p>Keeping of records</p>	
<p>1. The Agency ☒ eu-LISA ☒ shall keep records of all data processing operations within the Central System. These records shall show the purpose, date and time of access, the data transmitted, the data used for interrogation and the name of both the unit entering or retrieving the data and the persons responsible.</p>			

<p>2. The records referred to in paragraph 1 of this Article may be used only for the data protection monitoring of the admissibility of data processing as well as to ensure data security pursuant to Article 34. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year after the storage period referred to in Article ⇒ 17 ⇐ 12(1) and in Article 16(1) has expired, unless they are required for monitoring procedures which have already begun.</p>			
<p>3. For the purposes laid down in Article 1(1)(a) and (b), each Member State shall take the necessary measures in order to achieve the objectives set out in paragraphs 1 and 2 of this Article in relation to its national system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.</p>	<p>Amendment 127</p> <p>3. For the purposes laid down in Article 1(1)(a), (aa) and (b), each Member State shall take the necessary measures in order to achieve the objectives set out in paragraphs 1 and 2 of this Article in relation to its national system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.</p>		<p><i>Text agreed with the exception of the reference to the Article on resettled persons' data</i></p> <p>3. For the purposes laid down in Article 1(1)(a), [aa] and (b), each Member State shall take the necessary measures in order to achieve the objectives set out in paragraphs 1 and 2 of this Article in relation to its national system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.</p>


<i>Article 29 30</i>		<i>Article 30</i>	
Rights of of information of of the data subject		Rights of information of the data subject	Rights of information
1. A person covered by Article 9 10(1), Article 14 13(1) or Article 17 14(1) shall be informed by the Member State of origin in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand \Rightarrow in a concise, transparent, intelligible and easily accessible form, using clear and plain language \Leftarrow , of the following:	Amendment 128 1. A person covered by Articles 10(1), 12a , Article 13(1) or Article 14(1) shall be informed by the Member State of origin in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand in a concise, transparent, intelligible and easily accessible form, using clear and plain language, of the following:	1. In accordance with Chapter III of Regulation (EU) No. 2016/679 , a [...] person covered by Article 10(1), Article 13(1) or Article 14(1) shall be informed by the Member State of origin in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand in a concise, transparent, intelligible and easily accessible form, using clear and plain language, of the following:	<i>Text agreed pending the reference to the Article on resettled persons' data</i> 1. A person covered by Articles 10(1), [12a,] Article 13(1) or Article 14(1) shall be informed by the Member State of origin in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand in a concise, transparent, intelligible and easily accessible form, using clear and plain language, of the following:
(a) the identity of the controller within the meaning of Article 2(d) of Directive [.../EU] 95/46/EC and of his or her representative, if any \Rightarrow and the contact details of the data protection officer \Leftarrow ;		(a) the identity and contact details of the controller within the meaning of Article 4(7) of Regulation (EU) No. 2016/679 [...] and of his or her representative, if any and the contact details of the data protection officer;	<i>Confirmed by trilogue</i> (a) the identity and contact details of the controller within the meaning of Article 4(7) of Regulation (EU) No. 2016/679 [...] and of his or her representative, if any and the contact details of the data protection officer;
(b) the purpose for which his or her data will be processed in Eurodac, including a description	Amendment 129 (b) the purpose for which his	(b) the purpose for which his or her data will be processed in Eurodac and the legal basis of	<i>Text agreed with the exception of the square bracketed text</i>

of the aims of Regulation (EU) No [...] 604/2013 , in accordance with ⇒ Article 6 ⇐ thereof and an explanation in intelligible form, using clear and plain language , of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;	or her data will be processed in Eurodac, including a description of the aims of Regulation (EU) No [...] , in accordance with Article 6 thereof and, <i>where applicable, of the aims of Regulation (EU) XXX/XXX, and</i> an explanation in intelligible form of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;	processing , including a description of the aims of Regulation (EU) No XXX/XXX [Dublin Regulation] [...], in accordance with Article 6 thereof and an explanation in intelligible form of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;	(b) the purpose for which his or her data will be processed in Eurodac and the legal basis of processing , including a description of the aims of Regulation (EU) No XXX/XXX [Dublin Regulation] [...], in accordance with Article 6 thereof and <i>[where applicable, of the aims of Regulation (EU) XXX/XXX [Resettlement Regulation], and]</i> an explanation in intelligible form of the fact that Eurodac may be accessed by the Member States and Europol for law enforcement purposes;
(c) the recipients ⇒ or categories of recipients ⇐ of the data;	Amendment 130 (c) the recipients or categories of recipients of the data of the data;		<i>Confirmed by trilogue</i> (c) the recipients or categories of recipients of the data of the data, if any ;
(d) in relation to a person covered by Article 9 <u>10</u> (1) or 14 <u>13</u> (1) ⇒ or 14(1) ⇐ , the obligation to have his or her fingerprints taken;	Amendment 131 (d) in relation to a person covered by Article Articles 10(1) or, 12a, 13(1) or 14(1) , the obligation to have his or her fingerprints taken;	(d) in relation to a person covered by Article 10(1) or 13(1) or 14(1), the obligation to have his or her biometric data [...] taken;	<i>Confirmed by trilogue (pending agreement on reference to the Article on resettled persons' data)</i> (d) in relation to a person covered by Articles 10(1), [12a] , or 13(1) or 14(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 ;
(e) the period for which the			

data will be stored pursuant to Article 17;			
<p>(ef) the the existence of the the right ⇒ to request from the controller of access to data relating to him or her, and the right to request that inaccurate data relating to him or her be corrected ⇒ rectified ⇒ and the completion of incomplete personal data or or that unlawfully processed personal data relating to ⇒ concerning him or her be erased or restricted, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the national supervisory authorities referred to in Article 30 <u>32(1)</u>;</p>	<p>Amendment 132</p> <p>(f) the existence of the right to <i>object to the processing of personal data</i>, to request from the controller access to data relating to him or her, and the right to request that inaccurate data relating to him or her be rectified and the completion of incomplete personal data or that unlawfully processed personal data concerning him or her be erased or restricted, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the supervisory authorities referred to in Article 32(1);</p>		<p><i>Confirmed by trilogue</i></p> <p>(f) the existence of the right to request from the controller access to data relating to him or her, and the right to request that inaccurate data relating to him or her be rectified and the completion of incomplete personal data or that unlawfully processed personal data concerning him or her be erased or restricted, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the supervisory authorities referred to in Article 32(1);</p>
<p>(g) the right to lodge a complaint to the supervisory authority.</p>		<p>(g) the right to lodge a complaint to the national supervisory authority.</p>	<p><i>Confirmed by trilogue</i></p> <p>(g) the right to lodge a complaint to the supervisory authority.</p>
<p>2. In relation to a person covered by Article 9 <u>10</u>(1) or 14 <u>13</u>(1) ⇒ and 14(1) ⇒, the information referred to in paragraph 1 of this Article shall be provided at the time when his or her fingerprints</p>	<p>Amendment 133</p> <p>2. In relation to a person covered by Article Articles 10(1), 12a, 13(1) and 14(1), the information referred to in paragraph 1 of this Article shall be provided at the</p>	<p>2. In relation to a person covered by Article 10(1) or 13(1) and 14(1), the information referred to in paragraph 1 of this Article shall be provided at the time when his or her biometric data [...] are</p>	<p><i>Text agreed with the exception of the reference to the Article on resettled persons' data</i></p> <p>2. In relation to a person covered by Articles 10(1), [12a], 13(1) and 14(1), the information referred to in</p>

are taken.	time when his or her fingerprints are taken.	taken.	paragraph 1 of this Article shall be provided at the time when his or her biometric data are taken.
In relation to a person covered by Article 17(1), the information referred to in paragraph 1 of this Article shall be provided no later than at the time when the data relating to that person are transmitted to the Central System. That obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.			
Where a person covered by Article 9 10(1), Article 14 13(1) and Article 17 14(1) is a minor, Member States shall provide the information in an age-appropriate manner.	Amendment 134 Where a person covered by Article 10(1), Article 12a , Article 13(1) and Article 14(1) is a minor, Member States shall <i>ensure that that person understands the procedure by providing</i> the information in an age-appropriate manner, <i>both orally and in writing, using leaflets, infographics, demonstrations, or a combination of all three, which are specifically designed to explain the fingerprinting and facial image procedure to minors.</i>	Where a person covered by Article 10(1), Article 13(1) and Article 14(1) is a minor, Member States shall provide the information in an age-appropriate manner using leaflets and/or infographics and/or demonstrations specifically designed to explain the procedure to capture biometric data to minors.	<i>Informal outcome of technical discussion (with the exception of square brackets)</i> Where a person covered by Article 10(1), [Article 12a,] Article 13(1) and Article 14(1) is a minor, the information shall be provided by Member States in an age-appropriate manner. This information shall be provided, The procedure to capture biometric data shall be explained to minors by using leaflets, infographics, demonstrations, or a combination of any of the three, as appropriate, specifically designed to explain the

			procedure to capture biometric data to <u>for minors and in such a way as to ensure that the minor understands it.</u>
3. A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in ⇒ Article 6(2) ⇐ of Regulation (EU) No [.../...] 604/2013 shall be drawn up in accordance with the procedure referred to in Article 44(2) of that Regulation.		3. A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 6(2) of Regulation (EU) No XXX/XXX [Dublin Regulation] [...] shall be drawn up in accordance with the procedure referred to in Article 44(2) of that Regulation.	3. A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 6(2) of Regulation (EU) No XXX/XXX [Dublin 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 rights of the data subject, the possibility of assistance ⇒ information ⇐ by the	Amendment 135 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 <i>possible administrative sanctions under national law to</i>		<i>Confirmed by trilogue</i> 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 <i>administrative measures for ensuring compliance with providing</i>

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.	<i>which a person may be subject in case of non-compliance with the fingerprinting process or the process for capturing facial images, 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.</i>		<i>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.</i>
<u>Article 31</u>		Article 31	
⊗ Right of access to, rectification and erasure of personal data ⊗		Right of access to, rectification and erasure of personal data	<i>Under discussion</i> <u>Right of access to, rectification, completion and erasure of personal data, and of restriction of the processing thereof</u>
41. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, in each Member State any data subject may, in accordance with the laws, regulations and procedures of that State, exercise the rights provided for in Article 12 of Directive 95/46/EC ⇨ the data subject's rights of access, rectification and erasure shall be exercised in accordance ,with Chapter III of Regulation (EU) No. [.../2016]	Amendment 136 1. For the purposes laid down in Article 1(1)(a), <i>(aa)</i> and (b) of this Regulation, the data subject's rights of access, rectification and erasure shall be exercised in accordance ,with Chapter III of Regulation (EU) No. [.../2016] and applied as set out in this Article.	1. For the purposes laid down in Article 1(1)(a) and (b) of this Regulation, the data subject's rights of access, rectification and erasure shall be exercised in accordance ,with Chapter III and Articles 77 and 79 of Regulation (EU) No. 2016/679 [...] and applied as set out in this Article.	<i>Under discussion - EP suggestion based on EES text (link to AM 137)</i> 1. For the purposes laid down in Article 1(1)(a), <i>[(aa)]</i> and (b) of this Regulation, the data subject's rights of access <u>to</u> , rectification, <u>completion and erasure of personal data, and of restriction of the processing</u> shall be exercised in accordance with Chapter III of Regulation (EU) No. 2016/679 and applied as set out in this Article.

and applied as set out in this Article ↵ .			
Without prejudice to the obligation to provide other information in accordance with Article 12(a) of Directive 95/46/EC, ☒ 2. The right of access of ☒ the data subject ☒ in each Member State ☒ shall have ☒ include ☒ the right to obtain communication of the data relating to him or her recorded in the Central System and of the Member State which transmitted them to the Central System. Such access to data may be granted only by a Member State.	<p>Amendment 137</p> <p>2. The right of access of the data subject in each Member State shall include the right to obtain communication of the data relating to him or her recorded in the Central System and of the Member State which transmitted them to the Central System. Such access to data may be granted only by a Member State. <i>For the purposes laid down in Article 1(1), in each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The Member State that transmitted such data shall correct or erase it without excessive delay, in accordance with national law and practice.</i></p>		<p><i>Under discussion (see also EP suggestion in paragraph 1 + recital (49a))</i></p> <p>2. The right of access of the data subject in each Member State shall include the right to obtain communication of the data relating to him or her recorded in the Central System and of the Member State which transmitted them to the Central System. Such access to data may be granted only by a Member State.</p>
5. For the purposes laid down in Article 1(1), in each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be			

<p>carried out without excessive delay by the Member State which transmitted the data, in accordance with its laws, regulations and procedures.</p>			
<p>62. For the purposes laid down in Article 1(1), if the rights of correction <input checked="" type="checkbox"/> rectification <input checked="" type="checkbox"/> and erasure are exercised in a Member State other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of the Member State or States which transmitted the data so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the Central System.</p>			
<p>73. For the purposes laid down in Article 1(1), if it emerges that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall correct <input checked="" type="checkbox"/> rectify <input checked="" type="checkbox"/> or erase the data in accordance with Article 27 28(3). That Member State shall confirm in writing to the data subject without excessive delay that it has taken action to correct <input checked="" type="checkbox"/> ,</p>		<p>3. If it emerges that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall rectify or erase the data in accordance with Article 28(3). That Member State shall confirm in writing to the data subject that it has taken action to [...] rectify, complete, erase or restrict the processing of personal data relating to him or her.</p>	<p>3. If it emerges that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall rectify or erase the data in accordance with Article 28(3). That Member State shall confirm in writing to the data subject that it has taken action to rectify, complete, erase or restrict the processing of personal data relating to him or her.</p>

rectify, or complete, or erase or restrict the processing of or personal or data relating to him or her.			
84. For the purposes laid down in Article 1(1), If the Member State which transmitted the data does not agree that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject without excessive delay why it is not prepared to correct or erase the data.		4. If the Member State which transmitted the data does not agree that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject why it is not prepared to rectify [...] or erase the data.	4. If the Member State which transmitted the data does not agree that data recorded in the Central System are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject why it is not prepared to 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.			
95. Any request under paragraphs		5. Any request under	5. Any request under paragraphs

<p>4 1 and 5 2 of this Article for access, rectification or erasure shall contain all the necessary particulars to identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the data subject's rights referred to in paragraphs 4 1 and 5 2 and shall be erased immediately afterwards.</p>		<p>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.</p>	<p>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.</p>
<p>106. The competent authorities of the Member States shall cooperate actively to enforce promptly the data subject's rights laid down in paragraphs 5, 6 and 7 for rectification and erasure .</p>			
<p>117. Whenever a person requests access to data relating to him or her in accordance with paragraph 4, the competent authority shall keep a record in the form of a written document that such a request was made and how it was addressed, and shall make that document available to the national supervisory authorities without delay.</p>			
<p>12. For the purposes laid down in Article 1(1) of this Regulation, in</p>			


<p>each Member State, the national supervisory authority shall, on the basis of his or her request, assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his or her rights.</p>			
<p>138. For the purposes laid down in Article 1(1) of this Regulation, the national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall assist and, where requested, advise him or her in exercising <input checked="" type="checkbox"/> provide information to the data subject concerning the exercise of <input checked="" type="checkbox"/> his or her right to <input checked="" type="checkbox"/> request from the data controller access, <input checked="" type="checkbox"/> correct <input checked="" type="checkbox"/> rectification, <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> completion, <input checked="" type="checkbox"/> or erase <input checked="" type="checkbox"/> erasure <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> or restriction of the processing of <input checked="" type="checkbox"/> personal <input checked="" type="checkbox"/> data <input checked="" type="checkbox"/> concerning him or her <input checked="" type="checkbox"/> . Both national <input checked="" type="checkbox"/> The <input checked="" type="checkbox"/> supervisory authorities shall cooperate to this end <input checked="" type="checkbox"/> in accordance with Chapter VII of Regulation (EU) [.../2016] <input checked="" type="checkbox"/> . Requests for such assistance may</p>		<p>8. The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall, where requested, provide information to the data subject concerning the exercise of his or her right to request from the data controller access, rectification, completion, erasure or restriction of the processing of personal data concerning him or her. The supervisory authorities shall cooperate in accordance with Chapter VII of Regulation (EU) 2016/679 [...].</p>	<p>8. The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall, where requested, provide information to the data subject concerning the exercise of his or her right to request from the data controller access, rectification, completion, erasure or restriction of the processing of personal data concerning him or her. The supervisory authorities shall cooperate in accordance with Chapter VII of Regulation (EU) 2016/679.</p>

<p>be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data.</p>			
<p>14. In each Member State any person may, in accordance with the laws, regulations and procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he or she is refused the right of access provided for in paragraph 4.</p>			
<p>15. Any person may, in accordance with the laws, regulations and procedures of the Member State which transmitted the data, bring an action or, if appropriate, a complaint before the competent authorities or courts of that State concerning the data relating to him or her recorded in the Central System, in order to exercise his or her rights under paragraph 5. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject in accordance with paragraph 13 shall subsist</p>			

throughout the proceedings.			
<i>Article 30 32</i>		<i>Article 32</i>	
Supervision by the national supervisory authorities		Supervision by the national supervisory authorities	
<p>1. For the purposes laid down in Article 1(1) of this Regulation, each Member State shall provide that the national supervisory authority or authorities of each Member State designated pursuant to Article 41 28(1) of Directive 95/46/EC referred to in Article [46(1)] of Regulation (EU) [.../2016] shall monitor independently, in accordance with its respective national law, the lawfulness of the processing, in accordance with this Regulation, of personal data by the Member State in question for the purposes laid out in Article 1(1)(a) and (b), including their transmission to the Central System.</p>	<p>Amendment 138</p> <p>1. each Each Member State shall provide that The supervisory authority or authorities of each Member State designated pursuant to Article 41 of Directive referred to in Article [46(1)] of Regulation (EU) [.../2016] 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), (aa) and (b), including their transmission to the Central System.</p>	<p>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) and (b), including their transmission to the Central System.</p>	<p><i>Text agreed with the exception of the reference to the square bracketed part on resettled persons' data</i></p> <p>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), [(aa)] and (b), including their transmission to the Central System.</p>
<p>2. Each Member State shall ensure that its national supervisory authority has access to advice from persons with sufficient knowledge of fingerprint data.</p>		<p>2. Each Member State shall ensure that its national supervisory authority has access to advice from persons with sufficient knowledge of biometric [...] data.</p>	<p>2. Each Member State shall ensure that its national supervisory authority has access to advice from persons with sufficient knowledge of biometric data.</p>

<i>Article 31 33</i>		<i>Article 33</i>	
Supervision by the European Data Protection Supervisor		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 <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> the Agency , are carried out in accordance with Regulation (EC) No 45/2001 and with this Regulation.			
2. The European Data Protection Supervisor shall ensure that an audit of the Agency's <input checked="" type="checkbox"/> eu-LISA's <input checked="" type="checkbox"/> 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, <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> the Agency , and the national supervisory authorities. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall be given an opportunity to make comments before the report is adopted.			

<i>Article 32 34</i>		<i>Article 34</i>	
Cooperation between national supervisory authorities and the European Data Protection Supervisor		Cooperation between national supervisory authorities and the European Data Protection Supervisor	
1. The national supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their respective competences, cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of Eurodac.			
2. Member States shall ensure that every year an audit of the processing of personal data for the purposes laid down in Article 1(2)(c) is carried out by an independent body, in accordance with Article 33(2) 35(1), including an analysis of a sample of reasoned electronic requests.			
The audit shall be attached to the annual report of the Member States referred to in Article 40(7) 42(8).			
3. The national supervisory			

<p>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.</p>			
<p>4. For the purpose laid down in paragraph 3, the national supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> every two years.</p>	<p>Amendment 139</p> <p>4. For the purpose laid down in paragraph 3, the national supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities, assessing the application of the data protection</p>		<p><i>Confirmed by trilogue (text based on a similar provision in VIS)</i></p> <p>4. For the purpose laid down in paragraph 3, the national supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the</p>

	<i>provisions of this Regulation, as well as the necessity and proportionality of access to Eurodac for law enforcement purposes, shall be sent to the European Parliament, the Council, the Commission and eu-LISA every years.</i>		<i>Commission and the Management Authority every two years. This report shall include a chapter of each Member State prepared by the National Supervisory Authority of that Member State.</i>
<i>Article 33 35</i>		<i>Article 35</i>	
Protection of personal data for law enforcement purposes		Protection of personal data for law enforcement purposes	
1. Each Member State shall provide that the provisions adopted under national law implementing Framework Decision 2008/977/JHA are also applicable to the processing of personal data by its national authorities for the purposes laid down in Article 1(2) of this Regulation.			
21. The ☒ supervisory authority or authorities of each Member State referred to in Article [39(1)] of Directive [2016/... /EU] shall ☒ monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States for the purposes laid down in		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	<i>Confirmed by trilogue</i> 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

Article 1(21)(c) of this Regulation, including their transmission to and from Eurodac, shall be carried out by the national supervisory authorities designated pursuant to Framework Decision 2008/977/JHA.		Article 1(1)(c) of this Regulation, including their transmission to and from Eurodac.	the purposes laid down in Article 1(1)(c) of this Regulation, including their transmission to and from Eurodac.
32. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA and shall be supervised by an independent external data protection supervisor. Articles 30, 31 and 32 of that Decision shall be applicable to the processing of personal data by Europol pursuant to this Regulation. The independent external data protection supervisor shall ensure that the rights of the individual are not violated.		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 [...]. [...]	<i>Confirmed by trilogue</i> 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 [...]. [...]
43. Personal data obtained pursuant to this Regulation from Eurodac for the purposes laid down in Article 1(21)(c) shall only be processed for the purposes of the prevention, detection or investigation of the specific case for which the data have been requested by a Member State or by Europol.			

<p>54. ☒ Without prejudice to Article [23 and 24] of Directive [2016/ .../EU], ☒ the Central System, the designated and verifying authorities and Europol shall keep records of the searches for the purpose of permitting the national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union data protection rules, including for the purpose of maintaining records in order to prepare the annual reports referred to in Article 40(7) 42(8). Other than for such purposes, personal data, as well as the records of the searches, shall be erased in all national and Europol files after a period of one month, unless the data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol.</p>		<p>4. Without prejudice to Article [23 and 24] of Directive (EU) 2016/680, the Central System, the designated and verifying authorities and Europol shall keep records of the searches for the purpose of permitting the national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union data protection rules, including for the purpose of maintaining records in order to prepare the annual reports referred to in Article 42(8). Other than for such purposes, personal data, as well as the records of the searches, shall be erased in all national and Europol files after a period of one month, unless the data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol.</p>	<p>4. Without prejudice to Article [23 and 24] of Directive (EU) 2016/680, the Central System, the designated and verifying authorities and Europol shall keep records of the searches for the purpose of permitting the national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union data protection rules, including for the purpose of maintaining records in order to prepare the annual reports referred to in Article 42(8). Other than for such purposes, personal data, as well as the records of the searches, shall be erased in all national and Europol files after a period of one month, unless the data are required for the purposes of the specific ongoing criminal investigation for which they were requested by a Member State or by Europol.</p>
<p><i>Article 34 36</i></p>		<p><i>Article 36</i></p>	
<p>Data security</p>		<p>Data security</p>	
<p>1. The Member State of origin shall ensure the security of the</p>			

data before and during transmission to the Central System.			
2. Each Member State shall, in relation to all data processed by its competent authorities pursuant to this Regulation, adopt the necessary measures, including a security plan, in order to:			
(a) physically protect the data, including by making contingency plans for the protection of critical infrastructure;			
(b) deny unauthorised persons access to ⇒ data-processing equipment and ⇐ national installations in which the Member State carries out operations in accordance with the purposes of Eurodac (⇐ equipment, access control and ⇐ checks at entrance to the installation);			
(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);			
(d) prevent the unauthorised input of data and the unauthorised inspection, modification or erasure of stored personal data (storage			

control);			
(e) prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);			
(e f) prevent the unauthorised processing of data in Eurodac and any unauthorised modification or erasure of data processed in Eurodac (control of data entry);			
(f g) ensure that persons authorised to access Eurodac have access only to the data covered by their access authorisation, by means of individual and unique user IDs and confidential access modes only (data access control);			
(g h) ensure that all authorities with a right of access to Eurodac create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data, and make those profiles and any other relevant information which those authorities may require for supervisory purposes available to the national supervisory		(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	<p><i>Confirmed by trilogue</i></p> <p>(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</p>

<p>authorities referred to in <input checked="" type="checkbox"/> Chapter VI of Regulation (EU) No. [...] /2016 <input checked="" type="checkbox"/> Article 28 of Directive 95/46/EC and in <input checked="" type="checkbox"/> Chapter VI of Article of Directive [2016/.../EU] <input checked="" type="checkbox"/> Article [...] of Directive [2016/.../EU] <input checked="" type="checkbox"/> 25 of Framework Decision 2008/977/JHA without delay at their request (personnel profiles);</p>		<p>referred to in Article 51 [...] of Regulation (EU) No. 2016/679 [...] and in [...] Article 41 of Directive (EU) 2016/680 [...] without delay at their request (personnel profiles);</p>	<p>[...] of Regulation (EU) No. 2016/679 [...] and in [...] Article 41 of Directive (EU) 2016/680 [...] without delay at their request (personnel profiles);</p>
<p>(hi) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);</p>			
<p>(ij) 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);</p>			
<p>(ik) prevent the unauthorised reading, copying, modification or erasure <input checked="" type="checkbox"/> deletion <input checked="" type="checkbox"/> 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</p>			

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);			
(kn) 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 (kn) ⇒ (k) ⇐ that might indicate the occurrence of a security incident.			
3. Member States shall inform the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> of security incidents detected on their	Amendment 140 3. Member States shall inform eu-LISA of security	3. Member States shall inform eu-LISA of security incidents detected on their systems without	<i>Under discussion - Rapporteur's proposal</i> 2a. Europol shall, in relation to all

<p>systems ⇒ without prejudice to the notification and communication of a personal data breach pursuant to [Articles 31 and 32] of Regulation (EU) No [.../2016] respectively [Articles 28 and 29] ⇐ . The Agency ☒ eu-LISA ☒ shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents. The Member States concerned, the Agency ☒ eu-LISA ☒ and Europol shall collaborate during a security incident.</p>	<p>incidents detected on their systems without prejudice to the notification and communication of a personal data breach pursuant to [Articles 31 and 32 33 and 34] of Regulation (EU) No [.../2016] respectively [Articles 28 and 29] 679/2016. In particular, data subjects shall be notified by eu-LISA without undue delay when a security incident is likely to result in a high risk to their rights and freedoms. eu-LISA shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents. The Member States concerned, eu-LISA and Europol shall collaborate during a security incident.</p>	<p>prejudice to the notification and communication of a personal data breach pursuant to Articles 33 [...] and 34 [...] of Regulation (EU) No 2016/679 and Articles 30 and 31 of Directive (EU) 2016/680 [...] respectively [...]. eu-LISA shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents. The Member States concerned, eu-LISA and Europol shall collaborate during a security incident.</p>	<p><i>data processed pursuant to this Regulation, adopt the necessary measures to ensure the security of the processing in accordance with Article 32 of Regulation 2016/794.</i></p> <p><i>Alternative wording for a new recital 48a:</i></p> <p><i>(48a) Regulation 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.</i></p> <p>3. Member States and Europol shall inform eu-LISA of security incidents detected on their systems without prejudice to the notification and communication of a personal data breach, pursuant to Articles 33 and 34 of Regulation (EU) No 2016/679 and Articles 30 and 31 of Directive (EU) 2016/680, and 34 of Regulation 2016/794 respectively. Eu-LISA shall inform <i>without undue delay</i> the Member States, Europol and the European Data Protection Supervisor in case of security incidents <i>detected on the system without prejudice to [Article 37 of Regulation 45/2001].</i> The Member States concerned, eu-</p>
--	--	---	---

			LISA and Europol shall collaborate during a security incident.
4. The Agency ☒ eu-LISA ☒ shall take the necessary measures in order to achieve the objectives set out in paragraph 2 as regards the operation of Eurodac, including the adoption of a security plan.			
<i>Article 35 37</i>		<i>Article 37</i>	
Prohibition of transfers of data to third countries, international organisations or private entities		Prohibition of transfers of data to third countries, international organisations or private entities	
1. Personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of [Article [...]2(b) of Directive [2016/.../EU] Framework Decision 2008/977/JHA].	Amendment 141 1. Personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Regulation (EU) 679/2016 and [Article [...]2(b) of Directive	1. Personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Article 3(2) [...] of Directive (EU) 2016/680 [...].	<i>Confirmed by trilogue</i> 1. Personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. This prohibition shall also apply if those data are further processed at national level or between Member States within the meaning of Article 4(2) of Regulation (EU) 2016/679 and Article 3(2) of Directive (EU) 2016/680.

	[2016/.../EU] (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(2)(1)(c) shall not be transferred to third countries if there is a serious <input checked="" type="checkbox"/> real <input checked="" type="checkbox"/> 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.	Amendment 142 2. Personal data which originated in a Member State and are exchanged between Member States following a hit obtained for the purposes laid down in Article 1(1)(c) shall not be transferred to third countries, including 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.		<i>Informal outcome of technical discussion</i> 2. Personal data which originated in a Member State and are exchanged between Member States following a hit obtained for the purposes laid down in Article 1(1)(c) shall not be transferred to third countries if there is a real risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights.
3. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1), particularly where that country is also the applicant's country of origin.	Amendment 143 3. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1) or Article 12a , particularly where that country is also the applicant's country of origin.	3. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1) [...].	<i>Text agreed with the exception of the reference to the Article on resettled persons' data</i> 3. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1) [or Article 12a] [...].
34. The prohibitions referred to in paragraphs 1 and 2 shall be without prejudice to the right of Member States to transfer such		4. The prohibitions referred to in paragraphs 1 and 2 shall be without prejudice to the right of Member States to transfer such	<i>Confirmed by trilogue</i> 4. The prohibitions referred to in paragraphs 1 and 2 shall be without

data ⇒ in accordance with Chapter V of Regulation (EU) No [...] /2016] respectively with the national rules adopted pursuant to Directive [2016/.../EU] ⇐ to third countries to which Regulation (EU) No [...] /...] 604/2013 applies.		data in accordance with Chapter V of Regulation (EU) No 2016/679 [...] respectively with the national rules adopted pursuant to Chapter V of Directive (EU) 2016/680 [...] to third countries to which Regulation (EU) No XXX/XXX [Dublin Regulation] [...] applies.	prejudice to the right of Member States to transfer such data in accordance with Chapter V of Regulation (EU) No 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) No XXX/XXX [Dublin Regulation] applies.
Article 38		Article 38	
Transfer of data to third countries for the purpose of return		Transfer of data to third countries for the purpose of return	
1. By way of derogation from Article 37 of this Regulation, the personal data relating to persons referred to in Articles 10(1), 13(2), 14(1) obtained by a Member State following a hit for the purposes laid down in Article 1(1)(a) or (b) may be transferred or made available to a third-country in accordance with Article 46 of Regulation (EU) No. [...] /2016], if necessary in order to prove the identity of third-country nationals for the purpose of return, only where the following conditions are satisfied:	Amendment 144 1. By way of derogation from Article 37 of this Regulation, the only the necessary personal data relating to persons referred to in Articles 10(1), 13(2), 14(1) obtained by a Member State following a hit for the purposes laid down in Article 1(1)(a) or (b) may be transferred or made available to a third-country in accordance with Article 46 Chapter V of Regulation (EU) No. [...] /2016]; 2016/679 , if necessary in order to prove the identity of third-country nationals or stateless persons for the purpose of return,	1. By way of derogation from Article 37 of this Regulation, the personal data relating to persons referred to in Articles 10(1), 13(2), 14(1) obtained by a Member State following a hit for the purposes laid down in Article 1(1)(a) or (b) may be transferred or made available to a third-country in accordance with Chapter V [...] of Regulation (EU) No. 2016/679 [...], if necessary in order to prove the identity of third-country nationals or stateless persons for the purpose of return [...].	<i>EP suggestion for a compromise:</i> <i>EP would agree with deletion of AM 144, 145 and 146 if the Council agrees to go back to the COM text on Art. 38(1)</i>

	only where the following conditions are satisfied:		
(b) the third country explicitly agrees to use the data only for the purpose for which they were provided and to what is lawful and necessary to secure the purposes laid down in Article 1(1)(b) and to delete that data where it is no longer justified to keep it;		[...]	<p><i>EP suggestion for a compromise:</i></p> <p><i>EP would agree with deletion of AM 144, 145 and 146 if the Council agrees to go back to the COM text on Art. 38(1)</i></p>
(c) the Member State of origin which entered the data in the Central System has given its consent and the individual concerned has been informed that his or her personal information may be shared with the authorities of a third-country.	<p>Amendment 145</p> <p>(c) the Member State of origin which entered the data in the Central System has given its consent and the individual concerned has been informed that his or her personal information will be shared with the authorities of that third-country.</p>	[...]	<p><i>EP suggestion for a compromise:</i></p> <p><i>EP would agree with deletion of AM 144, 145 and 146 if the Council agrees to go back to the COM text on Art. 38(1)</i></p>
	<p>Amendment 146</p> <p><i>1a. 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)(a) and (b) shall not be transferred to third countries if there is a real risk that, as a result</i></p>		<p><i>EP suggestion for a compromise:</i></p> <p><i>EP would agree with deletion of AM 144, 145 and 146 if the Council agrees to go back to the COM text on Art. 38(1)</i></p>

	<i>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.</i>		
2. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1), particularly where that country is also the applicant's country of origin.	Amendment 147 2. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1); particularly where that country is also the applicant's country of origin.	2. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1) [...].	2. No information regarding the fact that an application for international protection has been made in a Member State shall be disclosed to any third-country for persons related to Article 10(1).
	Amendment 148 <i>2a. Ultimate responsibility for the processing of personal data shall lie with the Member States, which are considered to be 'controllers' within the meaning of Regulation (EU) 2016/679.</i>		<i>Informal outcome of technical discussion</i> Deletion
3. A third-country shall not have direct access to the Central System to compare or transmit fingerprint data or any other personal data of a third-country national or stateless person and shall not be granted access via a		3. A third-country shall not have direct access to the Central System to compare or transmit biometric [...] data or any other personal data of a third-country national or stateless person and shall not be granted access via a	3. A third-country shall not have direct access to the Central System to compare or transmit biometric data or any other personal data of a third-country national or stateless person and shall not be granted access via a Member State's designated National

Member State's designated National Access Point.		Member State's designated National Access Point.	Access Point.
<i>Article 36 39</i>		<i>Article 39</i>	
Logging and documentation		Logging and documentation	
1. Each Member State and Europol shall ensure that all data processing operations resulting from requests for comparison with Eurodac data for the purposes laid down in Article 1(2)(1)(c) are logged or documented for the purposes of checking the admissibility of the request, monitoring the lawfulness of the data processing and data integrity and security, and self-monitoring.			
2. The log or documentation shall show in all cases:			
(a) the exact purpose of the request for comparison, including the concerned form of a terrorist offence or other serious criminal offence and, for Europol, the exact purpose of the request for comparison;			
(b) the reasonable grounds given not to conduct comparisons with other Member States			

under Decision 2008/615/JHA, in accordance with Article 20 <u>21</u> (1) of this Regulation;			
(c) the national file reference;			
(d) the date and exact time of the request for comparison by the National Access Point to the Central System;			
(e) the name of the authority having requested access for comparison, and the person responsible who made the request and processed the data;			
(f) where applicable, the use of the urgent procedure referred to in Article 19(3) <u>20</u> (4) and the decision taken with regard to the ex-post verification;			
(g) the data used for comparison;			
(h) in accordance with national rules or with Decision 2009/371/JHA, the identifying mark of the official who carried out the search and of the official who ordered the search or supply.		(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.	(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.
3. Logs and documentation shall be used only for monitoring the			

<p>lawfulness of data processing and for ensuring data integrity and security. Only logs <input checked="" type="checkbox"/> which do not <input checked="" type="checkbox"/> containing non-personal data may be used for the monitoring and evaluation referred to in Article 40 <u>42</u>. The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data processing and data integrity and security shall have access to these logs at their request for the purpose of fulfilling their duties <input checked="" type="checkbox"/> tasks <input checked="" type="checkbox"/>.</p>			
<p><i>Article 37 <u>40</u></i></p>		<p><i>Article 40</i></p>	
<p>Liability</p>		<p>Liability</p>	
<p>1. Any person who, or Member State which, has suffered <input checked="" type="checkbox"/> material or immaterial <input checked="" type="checkbox"/> damage as a result of an unlawful processing operation or any act incompatible with this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That State shall be exempted from its liability, in whole or in part, if it proves that it is not <input checked="" type="checkbox"/> in any way <input checked="" type="checkbox"/>.</p>			<p><i>Confirmed by trilogue</i></p> <p>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</p>

responsible for the event giving rise to the damage.			<p>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.</p>
2. If the failure of a Member State to comply with its obligations under this Regulation causes damage to the Central System, that Member State shall be liable for such damage, unless and insofar as the Agency ☒ eu-LISA ☒ or another Member State failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.			<p><i>Confirmed by trilogue</i></p> <p>2. If any failure of a Member State to comply with its obligations under this Regulation causes damage to the Central System, that Member State shall be held liable for such damage, unless and insofar as the Agency ☒ eu-LISA ☒ or another Member State failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.</p>
3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State ⇒ in accordance with Articles [75 and 76] of Regulation (EU) [.../2016] and Articles [52 and 53] of Directive [2016/.../EU] ⇐ .	Amendment 149	3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State in accordance with Articles [75 and 76] Chapter VIII of Regulation (EU) [.../2016] 2016/679 and	<p><i>Confirmed by trilogue</i></p> <p>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)</p>

	Articles [52 and 53] <i>Chapter VIII</i> of Directive [2016/.../EU] (EU) 2016/680 concerning remedies, liabilities and penalties.	2016/680 [...].	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 IX	
		OPERATIONAL MANAGEMENT OF DUBLINET AND AMENDMENTS TO REGULATION (EU) NO 1077/2011	<i>Rapporteur's proposal</i> OPERATIONAL MANAGEMENT OF DUBLINET
	Amendment 150 <i>Article 40a</i>	Article 40a	<i>Confirmed by trilogue</i> Article 40a ⁵³
	<i>Operational management of DubliNet and related tasks</i>	Operational Management of DubliNet and related tasks	Operational Management of DubliNet and related tasks
	1. <i>Eu-LISA shall operate and manage a separate secure electronic transmission channel between the authorities of Member States known as the 'DubliNet' communication</i>	1. A separate secure electronic transmission channel between the authorities of Member States known as the 'DubliNet' communication network set-up under Article 18	1. A separate secure electronic transmission channel between the authorities of Member States known as the 'DubliNet' communication network set-up under Article 18 of Regulation (EC)

⁵³ If the eu-LISA regulation is to be adopted prior to the adoption of the EUODAC Regulation, the text of Articles 40a and 40b of the EUODAC Regulation concerning the DubliNet and its operational management by the eu-LISA, as agreed, should be included exclusively in the eu-LISA Regulation.

	<i>network established by Article 18 of Commission Regulation (EC) No 1560/2003⁵⁴ for the purposes set out in Articles 32, 33 and 46 of Regulation (EU) No ...[Dublin IV].</i>	of Regulation (EC) No. 1560/2003 for the purposes set out in Articles 32, 33 and 46 of Regulation (EU) No. XXX/XXX [Dublin Regulation] [...] shall be operated and managed by eu-LISA.	No. 1560/2003 for the purposes set out in Articles 32, 33 and 46 of Regulation (EU) No. XXX/XXX [Dublin Regulation] [...] shall be operated and managed by eu-LISA.
	2. The operational management of DubliNet shall consist of all the tasks necessary to ensure its availability five days a week during normal business hours.	2. The operational management of DubliNet shall consist of all the tasks necessary to ensure the availability of DubliNet, five days a week during normal business hours.	2. The operational management of DubliNet shall consist of all the tasks necessary to ensure the availability of DubliNet, five days a week during normal business hours.
	3. Eu-LISA shall be responsible for the following tasks relating to DubliNet:	3. eu-LISA shall be responsible for the following tasks relating to DubliNet:	3. eu-LISA shall be responsible for the following tasks relating to DubliNet:
	(a) providing technical support to Member States by way of a helpdesk, five days a week during normal business hours, including in relation to problems concerning communication, email encryption and decryption, and problems arising from the signature of forms;	(a) technical support to Member States by way of a helpdesk five days a week during normal business hours, including problems relating to communications, email encryption and decryption, and problems arising from signature of forms.	(a) technical support to Member States by way of a helpdesk five days a week during normal business hours, including problems relating to communications, email encryption and decryption, and problems arising from signature of forms.
	(b) providing IT security services;	(b) provision of IT security services for DubliNet;	(b) provision of IT security services for DubliNet;

⁵⁴

Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ L 222, 5.9.2003, p. 3).

	<i>(c) managing, registering and renewing digital certificates used for encrypting and signing DubliNet e-mail messages;</i>	(c) management, registration and renewal of the digital certificates used for encrypting and signing DubliNet e-mail messages;	(c) management, registration and renewal of the digital certificates used for encrypting and signing DubliNet e-mail messages;
	<i>(d) the technical evolution of DubliNet;</i>	(d) technical evolution of DubliNet;	(d) technical evolution of DubliNet;
	<i>(e) contractual matters.</i>	(e) contractual matters.	(e) contractual matters.
	<i>4. 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 DubliNet.</i>	4. The Agency shall ensure, in cooperation with the Member States, that at all times the best available and most secure technology and techniques, subject to a cost-benefit analysis, are used for DubliNet.	4. The Agency shall ensure, in cooperation with the Member States, that at all times the best available and most secure technology and techniques, subject to a cost-benefit analysis, are used for DubliNet.
	Amendment 151 <i>CHAPTER VIIIa</i>		<i>Confirmed by trilogue</i> <i>CHAPTER IXa</i>
	<i>AMENDMENTS TO REGULATION (EU) NO 1077/2011</i>		<i>Confirmed by trilogue</i> <i>AMENDMENTS TO REGULATION (EU) NO 1077/2011</i>
	Amendment 152 <i>Article 40 b</i>	Article 40b	<i>Confirmed by trilogue</i> Article 40b
	<i>Regulation (EU) No 1077/2011 is amended as follows:</i>	Amendments to Regulation (EU) No 1077/2011	<i>Confirmed by trilogue</i> Amendments to Regulation (EU)

			No 1077/2011
		Regulation (EU) No 1077/2011 is amended as follows:	<i>Confirmed by trilogue</i> Regulation (EU) No 1077/2011 is amended as follows:
	(1) In Article 1(2), the following subparagraph is added:	1. Article 1(2) is replaced by the following text:	1. Article 1(2) is replaced by the following text:
	<i>"The Agency shall also be responsible for the operational management of a separate secure electronic transmission channel between the authorities of Member States, known as the 'DubliNet' communication network, established by Article 18 of Commission Regulation (EC) No 1560/2003, for the exchange of information under Regulation (EU) No...⁵⁵[Dublin IV].</i>	"2. The Agency shall be responsible for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS),Eurodac, [the Entry Exit System (EES) established by XXX/XXX [EES Regulation]], and the DubliNet network established by Article 18 of Commission Regulation (EC) No 1560/2003⁵⁶ (DubliNet)."	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> "2. The Agency shall be responsible for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac, [the Entry Exit System (EES) established by XXX/XXX [EES Regulation]], and the DubliNet network established by

⁵⁵ Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ L 222, 5.9.2003, p. 3).".

⁵⁶ Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ L 222, 5.9.2003, p. 3).

			Article 18 of Commission Regulation (EC) No 1560/2003⁵⁷ (DubliNet)."
	(2) The following Article is inserted:	2. In Regulation 1077/2011, after Article 5 the following Article is added:	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> 2. The following Article is inserted:
	"Article 5a	"Article 5c	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> "Article 5a
	Tasks relating to DubliNet	Tasks relating to DubliNet	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> Tasks relating to DubliNet
	1. In relation to DubliNet, the Agency shall perform:	1. In relation to DubliNet, the Agency shall perform:	1. In relation to DubliNet, the Agency shall perform:
	(a) the tasks conferred on it by Article [...] of Regulation (EU).../[Eurodac];	(a) the tasks conferred on it by Regulation (EU) No XXX/XXX [Dublin Regulation];	<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> (a) the tasks conferred on it by Article [...] of Regulation

⁵⁷

Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (OJ L 222, 5.9.2003, p. 3).

			(EU).../...[Eurodac];
	(b) tasks relating to training on the technical use of DubliNet."	(b) tasks relating to training on the technical use of DubliNet."	(b) tasks relating to training on the technical use of DubliNet."
CHAPTER VIII			
AMENDMENTS TO REGULATION (EU) NO 1077/2011			
Article 38			
Amendments to Regulation (EU) No 1077/2011			
Regulation (EU) No 1077/2011 is amended as follows:			
(1) Article 5 is replaced by the following:			
"Article 5			
Tasks relating to Eurodac			
In relation to Eurodac, the Agency shall perform:			
(a) the tasks conferred on it by			

Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes⁵⁸; and			
(b) tasks relating to training on the technical use of Eurodac."»			
(2) Article 12(1) is amended as follows:			
(a) points (u) and (v) are replaced by the following:			
"(u) adopt the annual report on the activities of the Central System of Eurodac pursuant to Article 40(1)			

of Regulation (EU) No 603/2013;			
(v) make comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013 and ensure appropriate follow-up of those audits;"»			
(b) point (x) is replaced by the following:			
"(x) compile statistics on the work of the Central System of Eurodac pursuant to Article 8(2) of Regulation (EU) No 603/2013;"»			
(c) point (z) is replaced by the following:			
"(z) ensure annual publication of the list of units pursuant to Article 27(2) of Regulation (EU) No 603/2013;"»			
(3) Article 15(4) is replaced by the following:			
"4. Europol and Eurojust may attend the meetings of the Management Board as observers			

when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, is on the agenda.";			
(4) Article 17 is amended as follows:			
(a) in paragraph 5, point (g) is replaced by the following:			
"(g) without prejudice to Article 17 of the Staff Regulations, establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008 and Article 4(4) of Regulation (EU) No 603/2013;"			
(b) in paragraph 6, point (i) is replaced by the following:			
"(i) reports on the technical functioning of each large-scale IT			



system referred to in Article 12(1)(t) and the annual report on the activities of the Central System of Eurodac referred to in Article 12(1)(u), on the basis of the results of monitoring and evaluation."»			
(5) Article 19(3) is replaced by the following:			
"3. Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and Eurodac Advisory Groups."»			
CHAPTER IX		CHAPTER IX	
<i>FINAL PROVISIONS</i>		FINAL PROVISIONS	
<i>Article 39 41</i>		<i>Article 41</i>	
Costs		Costs	
1. The costs incurred in connection with the establishment and operation of the Central System and the Communication Infrastructure shall be borne by the general budget of the European	Amendment 153 1. The costs incurred in connection with the establishment and operation of the Central System and the Communication Infrastructure shall be borne by the		<i>Informal outcome of technical discussion</i> 1. The costs incurred in connection with the establishment and operation of the Central System and the Communication Infrastructure

Union.	general budget of the European Union, <i>in accordance with the principles of sound financial management.</i>		shall be borne by the general budget of the European Union.
2. The costs incurred by national access points and the costs for connection to the Central System shall be borne by each Member State.			<i>Confirmed by trilogue</i> 2. The costs incurred by [...]national access points and the Europol access point and their costs for connection to the Central System shall be borne by each Member State and Europol respectively.
	Amendment 154 <i>2a. In order to enable interoperability between the EES and Eurodac, eu-LISA shall establish a secure communication channel between the EES Central System and the Eurodac Central System. The two central systems shall be connected to allow for the transfer to Eurodac of the biometric data of third-country nationals registered in the EES where registration of those biometric data are required by this Regulation.</i>		<i>Informal outcome of technical discussion - to be confirmed by trilogue</i> Deletion
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(21)(c).			
<i>Article 40 42</i>		<i>Article 42</i>	
Annual report: monitoring and evaluation		Annual report: monitoring and evaluation	
1. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor an annual report on the activities of the Central System, including on its technical functioning and security. The annual report shall include information on the management and performance of Eurodac against pre-defined quantitative indicators for the objectives referred to in paragraph 2.			
2. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall ensure that procedures are in place to monitor the functioning of the Central System against objectives relating to output, cost-effectiveness and quality of			

service.			
3. For the purposes of technical maintenance, reporting and statistics, the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> shall have access to the necessary information relating to the processing operations performed in the Central System.			
4. By [2020] eu-LISA shall conduct a study on the technical feasibility of adding facial recognition software to the Central System for the purposes of comparing facial images. The study shall evaluate the reliability and accuracy of the results produced from facial recognition software for the purposes of EURODAC and shall make any necessary recommendations prior to the introduction of the facial recognition technology to the Central System.	<p>Amendment 155</p> <p>4. By [2020] eu-LISA shall conduct a study on the technical feasibility and added value of adding facial recognition software to the Central System for the purposes of comparing facial images 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 the Central System. <i>The study shall also include an impact assessment of the possible risks to the rights of privacy and human dignity, the rights of the child, as well as non-discrimination, as a result of using facial recognition</i></p>	<p>4. By [...] eu-LISA shall conduct a study on the technical feasibility of adding facial recognition software to the Central System for the purposes of comparing facial images. The study shall evaluate the reliability and accuracy of the results produced from facial recognition software for the purposes of EURODAC and shall make any necessary recommendations prior to the introduction of the facial recognition technology to the Central System.</p>	<p><i>Rapporteur's proposal</i></p> <p>4. By [2020] eu-LISA shall conduct a study on the technical feasibility and added value of adding facial recognition software to the Central System for the purposes of comparing facial images, <i>including of minors</i>. The study shall evaluate the reliability and accuracy of the results produced from facial recognition software for the purposes of EURODAC and shall make any necessary recommendations prior to the introduction of the facial recognition technology to the Central System. <i>The study shall take into account the views of other Union agencies, notably of the Fundamental Rights Agency, the European Data Protection Supervisor, relevant actors as well as academics.</i></p>

	<i>software. The study shall take into account the views of other Union agencies, the European Data Protection Supervisor, relevant actors as well as academics.</i>		
<p>45. By 20 July 2018 ⇒ [...] ⇐ and every four years thereafter, the Commission shall produce an overall evaluation of Eurodac, examining the results achieved against objectives and the impact on fundamental rights, including whether law enforcement access has led to indirect discrimination against persons covered by this Regulation, and assessing the continuing validity of the underlying rationale and any implications for future operations, and shall make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.</p>	<p>Amendment 156</p> <p>5. By [...] and every four years thereafter, the Commission shall produce an overall evaluation of Eurodac, <i>together with a full data protection and privacy impact assessment</i>, examining the results achieved against objectives and the impact on fundamental rights, including whether law enforcement access has led to indirect discrimination against persons covered by this Regulation, and assessing the continuing validity of the underlying rationale and any implications for future operations, and shall make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.</p>		<p><i>Informal outcome of technical discussion</i></p> <p>5. By [...] and every four years thereafter, the Commission shall produce an overall evaluation of Eurodac, examining the results achieved against objectives and the impact on fundamental rights, <i>in particular data protection and privacy rights</i>, including whether law enforcement access has led to indirect discrimination against persons covered by this Regulation, and assessing the continuing validity of the underlying rationale and any implications for future operations, and shall make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.</p>
<p>56. Member States shall provide the Agency ☒ eu-LISA ☒ and the Commission with the</p>			

information necessary to draft the annual report referred to in paragraph 1.			
67. The Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> , Member States and Europol shall provide the Commission with the information necessary to draft the overall evaluation provided for in paragraph 4 <u>5</u> . This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.			
78. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with Eurodac data for law enforcement purposes, containing information and statistics on:		8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of biometric [...] data with Eurodac data for law enforcement purposes, containing information and statistics on:	8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of biometric data with Eurodac data for law enforcement purposes, containing information and statistics on:
– the exact purpose of the comparison, including the type of terrorist offence or serious criminal offence,			
– grounds given for reasonable suspicion,			

– the reasonable grounds given not to conduct comparison with other Member States under Decision 2008/615/JHA, in accordance with Article 20 <u>21</u> (1) of this Regulation,			
– number of requests for comparison,			
– the number and type of cases which have ended in successful identifications, and			
– the need and use made of the exceptional case of urgency, including those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority.			
Member States' and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.			
89 . On the basis of Member States and Europol annual reports provided for in paragraph 7 <u>8</u> and in addition to the overall evaluation provided for in paragraph <u>4</u> <u>5</u> , the Commission shall compile an annual report on		9. [...]	<i>Under discussion</i>

law enforcement access to Eurodac and shall transmit it to the European Parliament, the Council and the European Data Protection Supervisor.			
<i>Article 41 43</i>		<i>Article 43</i>	
Penalties		Penalties	
Member States shall take the necessary measures to ensure that any processing of data entered in the Central System contrary to the purposes of Eurodac as laid down in Article 1 is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive.			
<i>Article 42 44</i>		<i>Article 44</i>	
Territorial scope		Territorial scope	
The provisions of this Regulation shall not be applicable to any territory to which [Regulation (EU) No 604/2013 does not apply].		The provisions of this Regulation shall not be applicable to any territory to which Regulation (EU) No XXX/XXX [Dublin Regulation] [...] does not apply.	The provisions of this Regulation shall not be applicable to any territory to which Regulation (EU) No XXX/XXX [Dublin Regulation] does not apply.

<i>Article 43 45</i>		<i>Article 45</i>	
Notification of designated authorities and verifying authorities		Notification of designated authorities and verifying authorities	
1. By ⇒ [...] ⇐ 20 October 2013 , each Member State shall notify the Commission of its designated authorities, of the operating units referred to in Article 5 6(3) and of its verifying authority, and shall notify without delay any amendment thereto.			
2. By ⇒ [...] ⇐ 20 October 2013 , Europol shall notify the Commission of its designated authority, of its verifying authority and of the National Access Point which it has designated, and shall notify without delay any amendment thereto.	Amendment 157 2. By [...] , Europol shall notify the Commission of its designated authority, of its verifying authority and of the National Access Point which it has designated , and <i>it</i> shall notify without delay any amendment thereto <i>without delay</i> .		<i>Confirmed by trilogue</i> 2. By [...], Europol shall notify the Commission of its designated authority <i>and</i> of its verifying authority [...] which it has designated , and shall notify without delay any amendment thereto.
3. The Commission shall publish the information referred to in paragraphs 1 and 2 in the <i>Official Journal of the European Union</i> on an annual basis and via an electronic publication that shall be available online and updated			

without delay.			
Article 44			
Transitional provision			
Data blocked in the Central System in accordance with Article 12 of Regulation (EC) No 2725/2000 shall be unblocked and marked in accordance with Article 18(1) of this Regulation on 20 July 2015.			
<i>Article 45 46</i>		<i>Article 46</i>	
Repeal		Repeal	
Regulation (EC) No 2725/2000 and Regulation (EC) No 407/2002 are <input checked="" type="checkbox"/> (EU) No 603/2013 is <input checked="" type="checkbox"/> repealed with effect from 20 July 2015 <input checked="" type="checkbox"/> [...] <input checked="" type="checkbox"/> .			
References to the repealed Regulations shall be construed as references to this Regulation and shall be read in accordance with the correlation table in <u>the Annex III</u> .			

<i>Article 46 47</i>		<i>Article 47</i>	
Entry into force and applicability		Entry into force and applicability	
This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i> .			
This Regulation shall apply from 20 July 2015 ⇒ [...] ⇐ .		This Regulation shall apply from [...] ⁵⁹ .	<i>Informal outcome of technical discussion</i> This Regulation shall apply from [<u>24 months from the date of entry into force of this Regulation</u>].
		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.	<i>Informal outcome of technical discussion</i> 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.
Articles 2(2), 32, 32 and, for the purposes referred to in Article 1(1)(a) and (b), Articles 28(4), 30 and 37 shall apply from the date referred to in Article 91(2) of		Articles 2(2), 32 [...] and, for the purposes referred to in Article 1(1)(a) and (b), Articles 28(4), 30 and 37 shall apply from the date referred to in Article 99 [...] (2) of	<i>Confirmed by trilogue</i> Articles 2(2), 32 [...] and, for the purposes referred to in Article 1(1)(a) and (b), Articles 28(4), 30 and 37

⁵⁹

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

Regulation (EU) [.../2016]. Until this date Articles 2(2), 27(4), 29, 30 and 35 of Regulation 603/2013 shall apply.		Regulation (EU) 2016/679 [...]. Until this date Articles 2(2), 27(4), 29, 30 and 35 of Regulation 603/2013 shall apply.	shall apply from the date referred to in Article 99 [...] (2) of Regulation (EU) 2016/679 [...]. Until this date Articles 2(2), 27(4), 29, 30 and 35 of Regulation 603/2013 shall apply.
Articles 2(4), 35, and for the purposes referred to in Article 1(1)(c), Article 28(4), 30, 37 and 40 shall apply from the date referred to in Article 62(1) of Directive [2016/.../EU]. Until this date Articles 2(4), 27(4), 29, 33, 35 and 37 of Regulation 603/2013 shall apply.		Articles 2(4), 35, and for the purposes referred to in Article 1(1)(c), Article 28(4), 30, 37 and 40 shall apply from the date referred to in Article 63 [...] (1) of Directive (EU) 2016/680 [...]. Until this date Articles 2(4), 27(4), 29, 33, 35 and 37 of Regulation 603/2013 shall apply.	<i>Confirmed by trilogue</i> Articles 2(4), 35, and for the purposes referred to in Article 1(1)(c), Article 28(4), 30, 37 and 40 shall apply from the date referred to in Article 63 [...] (1) of Directive (EU) 2016/680 [...]. Until this date Articles 2(4), 27(4), 29, 33, 35 and 37 of Regulation 603/2013 shall apply.
Comparisons of facial images with the use of facial recognition software as set out in Articles 15 and 16 of this Regulation shall apply from the date upon which the facial recognition technology has been introduced into the Central System. Facial recognition software shall be introduced into the Central System [<i>two years from the date of entry into force of this Regulation</i>]. Until that day, facial images shall be stored in the Central System as part of the data-subject's data sets and transmitted to a Member State following the comparison of fingerprints where			<i>Informal outcome of technical discussion</i> Comparisons of facial images with the use of facial recognition software as set out in Articles 15 and 16 of this Regulation shall apply from the date upon which the facial recognition technology has been introduced into the Central System. Facial recognition software shall be introduced into the Central System [<u>within one year from the conclusion of the study on the introduction of facial recognition software referred to in Article 42(4)</u>]. Until that day, facial images shall be stored in the Central System as part of the data-

there is a hit result.			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 the Agency <input checked="" type="checkbox"/> eu-LISA <input checked="" type="checkbox"/> as soon as they have made the technical arrangements to transmit data to the Central System <input checked="" type="checkbox"/> under Articles XX-XX <input checked="" type="checkbox"/> , and in any event no later than 20 July 2015 <input checked="" type="checkbox"/> [...] <input checked="" type="checkbox"/> .			<i>Informal outcome of technical discussion</i> Member States shall notify the Commission and eu-LISA as soon as they have made the technical arrangements to transmit data to the Central System under Articles XX-XX , no later than [<u><i>date of entry into force of this Regulation</i></u>] .
This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.			
Done at Brussels,			
<i>For the European Parliament</i> <i>For the Council</i>			
<i>The President</i> <i>The President</i>			



Council of the European Union
General Secretariat

**Interinstitutional files:
2016/0132 (COD)**

Brussels, 02 February 2018

WK 1308/2018 INIT

LIMITE

**ASILE
ENFOPOL
EURODAC**

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Delegations
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

With a view to their meeting on 7 February, Counsellors will find attached a 4-column table on the above subject.

Agreed text appears in green shading and text under discussion or where some further technical modifications are needed appears in orange shading.

WK 1308/2018 INIT

LIMITE

EN