



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 15 March 2013

7476/13

**Interinstitutional File:
2008/0242(COD)**

LIMITE

**EURODAC 4
CODEC 580
ENFOPOL 76**

NOTE

from:	General Secretariat of the Council
to:	Permanent Representatives Committee (Part II)
No. prev. doc.:	7022/13 EURODAC 3 CODEC 465 ENFOPOL 65
No. Cion prop.:	10638/12 EURODAC 3 ENFOPOL 157 CODEC 1503
Subject:	Amended 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 [.../...] (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 to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version) - Preparation for the fourth informal trilogue

1. The fourth amended proposal for a recast Regulation for Eurodac was adopted by the Commission on 30 May 2012, introducing the possibility for Member States' law enforcement authorities and Europol to consult the Eurodac data base for the purposes of prevention, detection, or investigation of terrorist offences and of other serious criminal offences. Following extensive examination by the competent Council bodies, the Permanent Representatives Committee gave its mandate to the then CY Pres on 10 October 2012 to start negotiations with the European Parliament. The LIBE Committee voted its Report on the recast proposal on 17 December 2012.

2. In the context of the ensuing negotiations between the Parliament and the Council, at political and technical level, considerable progress has been achieved, by way of provisional compromises. The results of these discussions are reflected at the fourth column of the annexed text. The Presidency considers that this progress has made an agreement possible on the basis of an overall package

The Presidency therefore seeks an amended mandate from the Committee which would allow it to negotiate with the Parliament, at the next informal trilogue to be held on 21 March 2013, with a view to reaching such an overarching compromise.

3. The package approach that the Presidency submits to the Committee is primarily based on possible compromises regarding the following issues, politically important issues for the two co-legislators:

- as regards the conditions of access to Eurodac data by designated authorities for law-enforcement purposes (Art. 20 (1) and 20 (1) (a) & (c), the Presidency is of the opinion that the provisional compromise accommodates the primary concerns of delegations, as this access is provided for without any disproportionate prior conditions;
- as regards the issue of transfers of data obtained pursuant to this Regulation to third countries (Art. 35 and Recital 33), the Presidency considers that the new compromise provides in a clear way for the cases where the transferring of data is prohibited as it falls under the relevant provisions of this Regulation and those which fall outside its scope and thus could be permissible. It is noted that, since the last JHA Counsellors meeting of 13 March 2013, a new version of Art. 35 and Recital 33 have been developed and inserted, as Presidency compromise suggestions, in the fourth column, and that Recital 33a is suggested to be deleted as its concept is covered by Art. 35(2);

- with regard to the period of storage of data of third-country nationals apprehended in connection with irregular crossing of the border of a Member State (Art. 16) and taking into account that both Parliament and Council have confirmed their support for a one or two-year storage period respectively, the Presidency proposes an 18-month storage period as the most viable compromise;
- in relation to the availability of data of beneficiaries of international protection for law-enforcement purposes (Art. 18), the Presidency will defend the Council position that this data should be available for five years after the data were first recorded in the Central System pursuant to Article 9(1). It is noted that the Parliament now accepts making this data available for asylum purposes for ten years and might be able to accept making it available for law enforcement purposes for three years from the time this international protection is granted, in line with the Qualification Directive.

In addition to the aforementioned issues, the discussions with the European Parliament have shown that the following points, which are of largely technical nature, will also need to be addressed in the context of an overall agreement with the European Parliament:

- with regard to the Parliament amendment providing for a transmission from the Central System of a maximum of five best fingerprints to the responsible designated authorities, (Art. 25(5)), the Presidency, on account of considerations that this could be prejudicial for the work of the law enforcement authorities and for the defence rights of the person concerned, suggests not accepting this amendment;
- in connection with the tentative compromise providing for an obligation for the responsible national administrations to make available to their national supervisory authorities the record they would be making of requests made by persons requesting the data relating to them (Article 29(9)), the Presidency considers that this is a compromise that could be taken on board, without creating any extra significant administrative burden;

- in relation with the compromise suggestions regarding the obligation for the Member States to carry out an audit, on an annual basis, of the processing of national data for law enforcement purposes, including the analysis of a sample of reasoned electronic requests - Art. 32 (1a), the Presidency considers that this could be acceptable, as it does not constitute an excessive administrative burden and the wording provides for sufficient flexibility;
- with regard to the Parliament's amendment concerning the provision of sufficient financial and professional resources for the national and European supervisory authorities in order to supervise the use and access to the Eurodac data (Art 32 (2a), the Presidency thinks that this is an issue that does not have a direct link with the subject-matter of the Eurodac Regulation and thus it should not be taken on board.

The Presidency considers that all the other remaining matters can be resolved at technical level based on the recommendations of the Presidency at the fourth column of the annexed table.

The Presidency invites the Permanent Representatives Committee to endorse the compromise package reflected in the fourth column of the attached table, with a view to mandating the Presidency to conduct the fourth informal trilogue on the Eurodac Recast Regulation with the European Parliament.

Amended 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 [.../...] (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 to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)

Commission proposal	EP amendments	Council position	comments / compromise suggestions
2008/0242 (COD)	2008/0242 (COD)	2008/0242 (COD)	
Amended proposal for a	Amended proposal for a	Amended proposal for a	
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	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 [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international	on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international	on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international	

<p>protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons 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</p> <p>(Recast version)</p>	<p>protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons 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</p> <p>(Recast version)</p>	<p>protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons 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</p> <p>(Recast version)</p>	
<p>THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,</p>	<p>THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,</p>	<p>THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,</p>	
<p>Having regard to the Treaty <u>on the Functioning of the European Union</u> establishing the European Community, and in particular Article 78 point (2)(e) 63 point (1)(a) ⇒ , Article 87 point (2)(a) and Article 88 point (2)(a) ⇐ thereof,</p>	<p>Having regard to the Treaty <u>on the Functioning of the European Union</u> establishing the European Community, and in particular Article 78 point (2)(e) 63 point (1)(a) ⇒ , Article 87 point (2)(a) and Article 88 point (2)(a) ⇐ thereof,</p>	<p>Having regard to the Treaty <u>on the Functioning of the European Union</u> establishing the European Community, and in particular Article 78 point (2)(e) 63 point (1)(a) ⇒ , Article 87 point (2)(a) and Article 88 point (2)(a) ⇐ thereof,</p>	

Having regard to the proposal from the Commission ¹ ,	Having regard to the proposal from the Commission ² ,	Having regard to the proposal from the Commission ³ ,	
Having regard to the opinion of the European Data Protection Supervisor ⁴ ,	Having regard to the opinion of the European Data Protection Supervisor ⁵ ,	Having regard to the opinion of the European Data Protection Supervisor ⁶ ,	
Having regard to the opinion of the European Parliament⁷	Having regard to the opinion of the European Parliament⁸	Having regard to the opinion of the European Parliament⁹	
<input checked="" type="checkbox"/> Acting in accordance with the ordinary legislative procedure, <input type="checkbox"/>	<input checked="" type="checkbox"/> Acting in accordance with the ordinary legislative procedure, <input type="checkbox"/>	<input checked="" type="checkbox"/> Acting in accordance with the ordinary legislative procedure, <input type="checkbox"/>	
Whereas:	Whereas:	Whereas:	
(1) A number of substantive changes are to be made to Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the	(1) A number of substantive changes are to be made to Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the	(1) A number of substantive changes are to be made to Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the	Identical

¹ COM(2012) XXX.

² COM(2012) XXX.

³ COM(2012) XXX.

⁴ OJ L 92 10.04.2010, p. 1

⁵ OJ L 92 10.04.2010, p. 1

⁶ OJ L 92 10.04.2010, p. 1

⁷ ~~OJ C 189, 7.7.2000, p. 105 and p. 227 and opinion delivered on 21 September 2000 (not yet published in the Official Journal).~~

⁸ ~~OJ C 189, 7.7.2000, p. 105 and p. 227 and opinion delivered on 21 September 2000 (not yet published in the Official Journal).~~

⁹ ~~OJ C 189, 7.7.2000, p. 105 and p. 227 and opinion delivered on 21 September 2000 (not yet published in the Official Journal).~~

<p>effective application of the Dublin Convention¹⁰ and 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 Convention¹¹. In the interest of clarity, those Regulations should be recast.</p>	<p>effective application of the Dublin Convention¹² and 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 Convention¹³. In the interest of clarity, those Regulations should be recast.</p>	<p>effective application of the Dublin Convention¹⁴ and 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 Convention¹⁵. In the interest of clarity, those Regulations should be recast.</p>	
<p>(1) Member States have ratified the Geneva Convention of 28 July 1951, as amended by the New York Protocol of 31 January 1967, relating to</p>	<p>(1) Member States have ratified the Geneva Convention of 28 July 1951, as amended by the New York Protocol of 31 January 1967, relating to</p>	<p>(1) Member States have ratified the Geneva Convention of 28 July 1951, as amended by the New York Protocol of 31 January 1967, relating to</p>	

¹⁰ OJ L 316, 15.12.2000, p. 1.

¹¹ OJ L 62, 5.3.2002, p. 1.

¹² OJ L 316, 15.12.2000, p. 1.

¹³ OJ L 62, 5.3.2002, p. 1.

¹⁴ OJ L 316, 15.12.2000, p. 1.

¹⁵ OJ L 62, 5.3.2002, p. 1.

the Status of Refugees.	the Status of Refugees.	the Status of Refugees.	
(2) Member States have concluded the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed in Dublin on 15 June 1990 (hereinafter referred to as "the Dublin Convention").	(2) Member States have concluded the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed in Dublin on 15 June 1990 (hereinafter referred to as "the Dublin Convention").	(2) Member States have concluded the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed in Dublin on 15 June 1990 (hereinafter referred to as "the Dublin Convention").	
(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, legitimately seek international protection in the Union.	(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, [...] seek international protection in the Union.	(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, legitimately seek international protection in the Union.	EP amendment accepted by Council.
(3) The European Council of 4 November 2004	(3) The European Council of 4 November 2004	(3) The European Council of 4 November 2004	Identical

<p>adopted The Hague Programme which sets 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 asylum procedure comprising common guarantees and a uniform status for refugees and the beneficiaries of subsidiary protection.</p>	<p>adopted The Hague Programme which sets 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 asylum procedure comprising common guarantees and a uniform status for refugees and the beneficiaries of subsidiary protection.</p>	<p>adopted The Hague Programme which sets 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 asylum procedure comprising common guarantees and a uniform status for refugees and the beneficiaries of subsidiary protection.</p>	
<p>(4) For the purposes of applying the Dublin Convention <input checked="" type="checkbox"/> Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State</p>	<p>(4) For the purposes of applying Regulation (EU) No [.../...] of the European Parliament and of the Council of ... [establishing the criteria and mechanisms for determining the Member</p>	<p>(4) For the purposes of applying the Dublin Convention <input checked="" type="checkbox"/> Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State</p>	<p>Technical amendments agreed</p>

<p>responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]¹⁶ ☒, it is necessary to establish the identity of applicants for asylum ⇒ international protection ⇐ and of persons apprehended in connection with the unlawful crossing of the external borders of the Community. It is also desirable, in order effectively to apply the Dublin Convention ☒ Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international</p>	<p>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 [.../...] [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</p>	<p>responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]¹⁷ ☒, it is necessary to establish the identity of applicants for asylum ⇒ 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 the Dublin Convention ☒ Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international</p>	
---	--	--	--

¹⁶ COM(2008)XXX.

* **OJ: Please insert the number, date and publication reference of the Dublin Regulation.** (The replacement of the term 'Community' by 'Union' applies throughout the text.)

¹⁷ COM(2008)XXX.

<p>protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>, and in particular points (c) and (e) (b) and (d) of Article 10(1)18(1) thereof, to allow each Member State to check whether an alien <input checked="" type="checkbox"/> third country national or stateless person <input checked="" type="checkbox"/> found illegally present <input checked="" type="checkbox"/> staying <input checked="" type="checkbox"/> on its territory has applied for <u>asylum</u> ⇒ international protection ⇐ in another Member State.</p>	<p>a third-country national or a stateless person]*, and in particular points (b) and (d) of Article 18(1) 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>protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>, and in particular points (c) and (e) (b) and (d) of Article 10(1)18(1) thereof, to allow each Member State to check whether an alien <input checked="" type="checkbox"/> third country national or stateless person <input checked="" type="checkbox"/> found illegally present <input checked="" type="checkbox"/> staying <input checked="" type="checkbox"/> on its territory has applied for <u>asylum</u> ⇒ international protection ⇐ in another Member State.</p>	
<p>(5) Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data.</p>	<p>(5) Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data.</p>	<p>(5) Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data.</p>	<p>Identical</p>
<p>(6) To this end, it is necessary to set up a system known as "<u>EurodacEURODAC</u>", consisting of a Central</p>	<p>(6) To this end, it is necessary to set up a system known as "<u>EurodacEURODAC</u>", consisting of a Central</p>	<p>(6) To this end, it is necessary to set up a system known as "<u>EurodacEURODAC</u>", consisting of a Central</p>	<p>Identical</p>

<p>Unit ⇒ System ⇐, to be established within the Commission and which will operate a computerised central database of fingerprint data, as well as of the electronic means of transmission between the Member States and the central database ⇒ Central System, hereinafter the "Communication Infrastructure". ⇐</p>	<p>Unit ⇒ System ⇐, to be established within the Commission and which will operate a computerised central database of fingerprint data, as well as of the electronic means of transmission between the Member States and the central database ⇒ Central System, hereinafter the "Communication Infrastructure". ⇐</p>	<p>Unit ⇒ System ⇐, to be established within the Commission and which will operate a computerised central database of fingerprint data, as well as of the electronic means of transmission between the Member States and the central database ⇒ Central System, hereinafter the "Communication Infrastructure". ⇐</p>	
<p>(7) The Hague Programme called for the improvement of access to existing data filing systems in the European 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>(7) The Hague Programme called for the improvement of access to existing data filing systems in the European 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>(7) The Hague Programme called for the improvement of access to existing data filing systems in the European 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>Identical</p>

<p>(8) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in EURODAC is necessary for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences. 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 Europol.</p>	<p><i>deleted</i></p>	<p>(8) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in EURODAC is necessary for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. 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 Europol.</p>	<p>The Recital is agreed to be maintained, with adjustment of its language to the 2008/633 Decision on the access to VIS by law enforcement authorities</p>
--	-----------------------	--	---

	<p>(8a) <i>The powers granted to law enforcement authorities to access EURODAC should be without prejudice to the right of the applicant for international protection to have his or her application processed in due course in accordance with the relevant law.</i></p> <p><i>Furthermore, obtaining a 'hit' from EURODAC and a subsequent procedure according to Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union¹⁸ should also be without prejudice to that right and should not be grounds for slowing down the process of</i></p>		<p>By way of compromise the Cion suggested the following wording (in bold,underline and strikethrough):</p> <p><i>The powers granted to law enforcement authorities to access EURODAC should be without prejudice to the right of the applicant for international protection to have his or her application processed in due course in accordance with the relevant law. Furthermore, <u>any subsequent follow-up after</u> obtaining a 'hit' from EURODAC and a subsequent procedure according to Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union¹⁹ should also be without prejudice to that right and should not be grounds for slowing down the process of examining the applicant's claim for international protection.</i></p>
--	--	--	---

¹⁸ OJ L 386, 29.12.2006, p. 89.

¹⁹ OJ L 386, 29.12.2006, p. 89.

	<i>examining the applicant's claim for international protection.</i>		The compromise suggestion is provisionally agreed.
(9) The Commission outlined in its Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs ²⁰ of 24 November 2005 that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. In this Communication the	(9) The Commission outlined in its Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs ²¹ of 24 November 2005 that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. In this Communication the	(9) The Commission outlined in its Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs ²² of 24 November 2005 that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. In this Communication the	Identical

²⁰ COM(2005) 597, 24.11.2005.

²¹ COM(2005) 597, 24.11.2005.

²² COM(2005) 597, 24.11.2005.

<p>Commission also found that the proportionality principle requires that EURODAC be queried for these purposes only once 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>Commission also found that the proportionality principle requires that EURODAC be queried for these purposes only once 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>Commission also found that the proportionality principle requires that EURODAC be queried for these purposes only once 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>(10) Moreover, Europol has a key role with respect to cooperation between Member States' authorities in the field of cross-border crime</p>	<p>(10) Moreover, Europol has a key role with respect to cooperation between Member States' authorities in the field of cross-border crime</p>	<p>(10) Moreover, Europol has a key role with respect to cooperation between Member States' authorities in the field of cross-border crime</p>	<p>Identical</p>

<p>investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to EURODAC data within the framework of its tasks and in accordance with the Decision establishing the European Police Office (Europol) No (2009/371/JHA).²³</p>	<p>investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to EURODAC data within the framework of its tasks and in accordance with the Decision establishing the European Police Office (Europol) No (2009/371/JHA).²⁴</p>	<p>investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to EURODAC data within the framework of its tasks and in accordance with the Decision establishing the European Police Office (Europol) No (2009/371/JHA).²⁵</p>	
	<p><i>(10a) Access to EURODAC data by Europol should be allowed only in specific cases, under specific circumstances and under strict conditions.</i></p>		<p>By way of compromise the wording of this draft Recital would read:</p> <p>"Requests for comparison of Eurodac data by Europol should be allowed only in specific cases..."</p> <p>Compromise agreed</p>
<p>(11) Since EURODAC has been established to facilitate the application</p>	<p>(11) Since EURODAC has been established to facilitate the application</p>	<p>(11) Since EURODAC has been established to facilitate the application</p>	

²³ OJ L 121, 15.5.2009, p. 37

²⁴ OJ L 121, 15.5.2009, p. 37

²⁵ OJ L 121, 15.5.2009, p. 37

<p>of Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], access to EURODAC for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences constitutes a change of the original purpose of EURODAC, which interferes with the right to respect the private life of individuals whose personal data are processed in EURODAC. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it</p>	<p>of Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], access to EURODAC for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences constitutes a change of the original purpose of EURODAC, which interferes with the right to respect the private life of individuals whose personal data are processed in EURODAC. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it</p>	<p>of Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], access to EURODAC for the purposes of preventing, detecting and of investigating terrorist offences and of other serious criminal offences constitutes a change of the original purpose of EURODAC, which interferes with the right to respect the private life of individuals whose personal data are processed in EURODAC. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to</p>	<p>Council agreed to replace the "and" at the Council text by "or" and the "of" by "or of" (throughout the draft Regulation)</p>
---	---	---	--

<p>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 attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.</p>	<p>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 attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.</p>	<p>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 attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.</p>	
<p>(12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The</p>	<p>(12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The</p>	<p>(12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The</p>	

<p>possibility to compare a latent with the fingerprint data which is stored in EURODAC will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.</p>	<p>possibility to compare a latent with the fingerprint data which is stored in EURODAC <i>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</i> will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.</p>	<p>possibility to compare a latent with the fingerprint data which is stored in EURODAC will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.</p>	<p>Pres recommends acceptance of the EP amendment</p>
	<p><i>(12a) The results of the comparison should be immediately checked in the Member State of origin by a fingerprint expert. Final identification should be made by the Member State of origin in</i></p>		<p>EP will further consider its amendment given its overlapping with Recital 17 of the Council text</p>

	<i>cooperation with the Member States concerned, pursuant to Article 32 of Regulation (EU) No [.../...] of the European Parliament and of the Council [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] *</i>		Technical - reference should be made to Art. 34 of the Dublin Regulation
	(12b) <i>Information received from the Central System relating to other data found to be unreliable should be erased as soon as the unreliability of the data is established.</i>		Agreed to be deleted
(13) This Regulation also lays down the conditions under which requests for comparison of fingerprint	(13) This Regulation also lays down the conditions under which requests for comparison of fingerprint	(13) This Regulation also lays down the conditions under which requests for comparison of fingerprint	

* *OJ: Please insert the number, date and publication reference of the Dublin Regulation.*

<p>data with EURODAC data for the purposes of preventing, detecting or investigating terrorist offences and 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.</p>	<p>data with EURODAC data for the purposes of preventing, detecting or investigating terrorist offences and 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. <i>Those conditions should take into consideration in particular the fact that the Eurodac database registers fingerprint data of persons to whom a legal presumption applies that they have a clean criminal record.</i></p>	<p>data with EURODAC data for the purposes of preventing, detecting or investigating terrorist offences and 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.=</p>	<p>Cion suggested an alternative clearer wording for the EP amendment, along the following lines: "The strictness of these conditions reflect the fact that the Eurodac data base registers finger print data of persons who would not be presumed to have committed a serious criminal offence or a terrorist offence".</p> <p>The Cion compromise is agreed</p>
<p>(14) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to</p>	<p>(14) <i>With a</i> view of ensuring equal treatment for all applicants <i>for</i> and beneficiaries of international protection, as well as in order to</p>	<p>(14) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to</p>	<p>The compromise text, which is agreed, reads as follows: "With a view to ensuring equal treatment for all applicants and for beneficiaries international protection, as well as in order to</p>

<p>ensure consistency with current Union asylum <i>acquis</i>, in particular with Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted²⁶ and Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to extent the</p>	<p>ensure consistency with the current Union asylum <i>acquis</i>, in particular with <i>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 and for persons eligible for subsidiary protection, and for the content of the protection granted</i>²⁷ and Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by</p>	<p>ensure consistency with current Union asylum <i>acquis</i>, in particular with Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted²⁸ and Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to extent the</p>	<p>ensure consistency with the current Union asylum <i>acquis</i>, in particular with Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees and for persons eligible for subsidiary protection, and for the content of the protection granted²⁹ and Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to extend the scope of this Regulation in order to include applicants for subsidiary protection and persons enjoying subsidiary protection."</p>
---	--	---	--

²⁶ OJ L 304, 30.9.2004, p. 12.

²⁷ OJ L 337, 20.12.2011, p. 9.

²⁸ OJ L 304, 30.9.2004, p. 12.

²⁹ OJ L 337, 20.12.2011, p. 9.

	scope of this Regulation to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.	a third-country national or a stateless person], it is appropriate to <i>extend</i> the scope of this Regulation <i>in</i> order to include applicants for subsidiary protection and persons enjoying subsidiary protection.	scope of this Regulation to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.	
(15)	It is also necessary to require the Member States promptly to take ⇨ and transmit ⇨ fingerprints ⇨ data ⇨ of every applicant for asylum ⇨ international protection ⇨ and of every alien ⊗ third country national or stateless person ⊗ who is apprehended in connection with the irregular crossing of an external border of a Member State, if they are at least 14 years of age.	(15) It is also necessary to require the Member States promptly to take ⇨ and transmit ⇨ fingerprints ⇨ data ⇨ of every applicant for asylum ⇨ international protection ⇨ and of every alien ⊗ third country national or stateless person ⊗ who is apprehended in connection with the irregular crossing of an external border of a Member State, if they are at least 14 years of age.	(15) It is also necessary to require the Member States promptly to take ⇨ and transmit ⇨ fingerprints ⇨ data ⇨ of every applicant for asylum ⇨ international protection ⇨ and of every alien ⊗ third country national or stateless person ⊗ who is apprehended in connection with the irregular crossing of an external border of a Member State, if they are at least 14 years of age.	Identical
(16)	It is necessary to lay down precise rules on the transmission of such fingerprint data to the Central Unit	(16) It is necessary to lay down precise rules on the transmission of such fingerprint data to the Central Unit	(16) It is necessary to lay down precise rules on the transmission of such fingerprint data to the Central Unit	Identical

<p>⇒ System ⇐, the recording of such fingerprint data and other relevant data in the Central Unit</p> <p>⇒ System ⇐, their storage, their comparison with other fingerprint data, the transmission of the results of such comparison and the blocking ⇒ marking ⇐ and erasure of the recorded data. Such rules may be different for, and should be specifically adapted to, the situation of different categories of aliens ⊗ third country nationals or stateless persons ⊗.</p>	<p>⇒ System ⇐, the recording of such fingerprint data and other relevant data in the Central Unit</p> <p>⇒ System ⇐, their storage, their comparison with other fingerprint data, the transmission of the results of such comparison and the blocking ⇒ marking ⇐ and erasure of the recorded data. Such rules may be different for, and should be specifically adapted to, the situation of different categories of aliens ⊗ third country nationals or stateless persons ⊗.</p>	<p>⇒ System ⇐, the recording of such fingerprint data and other relevant data in the Central Unit</p> <p>⇒ System ⇐, their storage, their comparison with other fingerprint data, the transmission of the results of such comparison and the blocking ⇒ marking ⇐ and erasure of the recorded data. Such rules may be different for, and should be specifically adapted to, the situation of different categories of aliens ⊗ third country nationals or stateless persons ⊗.</p>	
---	---	---	--

	<p>(16a) <i>Member States should ensure the transmission of fingerprint data in an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. All authorities with right of access to Eurodac should invest in adequate training and in the necessary technological equipment. The authorities with right of access to Eurodac should inform the Agency of specific difficulties encountered with regard to the quality of data, in order to resolve them.</i></p>		<p>The EP amendment is agreed, on the basis of clarification (accepted by the EP) that it applies only to asylum purposes and not to law-enforcement cases, where latents are generally of significantly lower quality.</p>
	<p>(16b) <i>A temporary or permanent impossibility for an applicant for international protection to provide fingerprints ('failure to enrol') should not adversely affect the legal situation of that applicant.</i></p>		<p>Replaced by a new Recital that will also take the place of Arts. 9(2)(a) and 14(2)(a). This Recital reads as follows:</p> <p><i>"Any temporary or permanent impossibility to take and/or to transmit fingerprint data, due to</i></p>

			<i>reasons such as insufficient quality of the data for appropriate comparison, technical problems, reasons linked to protection of health or due to the fact that the data subject is unfit or unable to have his/her fingerprints taken owing to circumstances beyond his/her control, should not adversely affect the examination and the decision on the application for international protection lodged by this person."</i>
(17) Hits obtained from EURODAC should be verified by a fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by	(17) 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 [...] [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	(17) Hits obtained from EURODAC should be verified by a fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by	Both EP and Council amendments agreed; the compromise text will read: 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 [...] [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 the exact identification of

<p>a third-country national or a stateless person].</p>	<p>a third-country national or a stateless person] * .</p>	<p>a third-country national or a stateless person] and the exact identification of the criminal suspect or victim of crime whose data might be stored in EURODAC .</p>	<p>the criminal suspect or victim of crime whose data might be stored in EURODAC .</p>
<p>(18) Aliens ⊗ Third country nationals or stateless persons ⊗ who have requested asylum ⇒ international protection ⇐ in one Member State may have the option of requesting asylum ⇒ international protection ⇐ in another Member State for many years to come. Therefore, the maximum period during which fingerprint data should be kept by the Central Unit ⇒ System ⇐ should be of considerable length. Given that most aliens ⊗ third country nationals or stateless persons ⊗ who have</p>	<p>(18) Aliens ⊗ Third country nationals or stateless persons ⊗ who have requested asylum ⇒ international protection ⇐ in one Member State may have the option of requesting asylum ⇒ international protection ⇐ in another Member State for many years to come. Therefore, the maximum period during which fingerprint data should be kept by the Central Unit ⇒ System ⇐ should be of considerable length. Given that most aliens ⊗ third country nationals or stateless persons ⊗ who have</p>	<p>(18) Aliens ⊗ Third country nationals or stateless persons ⊗ who have requested asylum ⇒ international protection ⇐ in one Member State may have the option of requesting asylum ⇒ international protection ⇐ in another Member State for many years to come. Therefore, the maximum period during which fingerprint data should be kept by the Central Unit ⇒ System ⇐ should be of considerable length. Given that most aliens ⊗ third country nationals or stateless persons ⊗ who have</p>	<p>Identical</p>

* *OJ: Please insert the number, date and publication reference of the Dublin Regulation.*

<p>stayed in the Community <input checked="" type="checkbox"/> European Union <input checked="" type="checkbox"/> 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 conservation of fingerprint data.</p>	<p>stayed in the Community <input checked="" type="checkbox"/> European Union <input checked="" type="checkbox"/> 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 conservation of fingerprint data.</p>	<p>stayed in the Community <input checked="" type="checkbox"/> European Union <input checked="" type="checkbox"/> 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 conservation of fingerprint data.</p>	
<p>(19) The conservation period should be shorter in certain special situations where there is no need to keep fingerprint data for that length of time. Fingerprint data should be erased immediately once aliens <input checked="" type="checkbox"/> third country nationals or stateless persons <input checked="" type="checkbox"/> obtain citizenship of a Member State.</p>	<p>(19) The conservation period should be shorter in certain special situations where there is no need to keep fingerprint data for that length of time. Fingerprint data should be erased immediately once aliens <input checked="" type="checkbox"/> third country nationals or stateless persons <input checked="" type="checkbox"/> obtain citizenship of a Member State.</p>	<p>(19) The conservation period should be shorter in certain special situations where there is no need to keep fingerprint data for that length of time. Fingerprint data should be erased immediately once aliens <input checked="" type="checkbox"/> third country nationals or stateless persons <input checked="" type="checkbox"/> obtain citizenship of a Member State.</p>	<p>Identical</p>
<p>(20) It is appropriate to store data relating to those data subjects whose fingerprints were initially recorded in EURODAC upon lodging their</p>	<p>(20) It is appropriate to store data relating to those data subjects whose fingerprints were initially recorded in EURODAC upon lodging their</p>	<p>(20) It is appropriate to store data relating to those data subjects whose fingerprints were initially recorded in EURODAC upon lodging their</p>	<p>Identical</p>

<p>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>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>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>(21) The European Agency for the operational management of large-scale information systems in the area of freedom security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011³⁰ (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of EURODAC in</p>	<p>(21) The European Agency for the operational management of large-scale information systems in the area of freedom security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011³¹ (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of EURODAC in</p>	<p>(21) The European Agency for the operational management of large-scale information systems in the area of freedom security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011³² (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of</p>	<p>Technical - agreed</p>

³⁰ OJ L 286, 1.11.2011, p. 1.

³¹ OJ L 286, 1.11.2011, p. 1.

³² OJ L 286, 1.11.2011, p. 1.

<p>accordance with this Regulation and with certain tasks relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should have observer status at the meetings of the Management Board of the Agency, when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences</p>	<p>accordance with this Regulation and with certain tasks relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should have observer status at the meetings of the Management Board of the Agency, when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences</p>	<p>EURODAC in accordance with this Regulation and with certain tasks relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should have observer status at the meetings of the Management Board of the Agency, when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other</p>	
--	--	---	--

<p>is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of the Agency.</p>	<p>is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of the Agency.</p>	<p>serious criminal offences is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of the Agency.</p>	
<p>(22) 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 (15) (together referred to as the ‘Staff Regulations’), should apply to all staff working in the Agency on matters pertaining to this Regulation.</p>	<p>(22) 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 (15) (together referred to as the ‘Staff Regulations’), should apply to all staff working in the Agency on matters pertaining to this Regulation.</p>	<p>(22) 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 (15) (together referred to as the ‘Staff Regulations’), should apply to all staff working in the Agency on matters pertaining to this Regulation.</p>	<p>Identical</p>
<p>(23) It is necessary to lay down clearly the respective responsibilities of the Commission ⇒ and the Agency ⇐, in respect of the Central Unit ⇒ System ⇐ ⇒ and</p>	<p>(23) It is necessary to lay down clearly the respective responsibilities of the Commission ⇒ and the Agency ⇐, in respect of the Central Unit ⇒ System ⇐ ⇒ and</p>	<p>(23) It is necessary to lay down clearly the respective responsibilities of the Commission ⇒ and the Agency ⇐, in respect of the Central Unit ⇒ System ⇐ ⇒ and</p>	<p>Identical</p>

<p>the Communication Infrastructure ⇐, and of the Member States, as regards data use <u>processing</u>, data security, access to, and correction of, recorded data.</p>	<p>the Communication Infrastructure ⇐, and of the Member States, as regards data use <u>processing</u>, data security, access to, and correction of, recorded data.</p>	<p>the Communication Infrastructure ⇐, and of the Member States, as regards data use <u>processing</u>, data security, access to, and correction of, recorded data.</p>	
<p>(24) It is necessary to designate the competent Member States' authorities as well as the National Central Access Point through which the requests for comparison with EURODAC data are done 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 and investigation of terrorist offences as referred to in the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism³³ and of other serious criminal</p>	<p>(24) It is necessary to designate the competent Member States' authorities as well as the National Central Access Point through which the requests for comparison with EURODAC data are done 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 and investigation of terrorist offences as referred to in the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism³⁵ and of other serious criminal</p>	<p>(24) It is necessary to designate the competent Member States' authorities as well as the National Central 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 and investigation of terrorist offences as referred to in the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism³⁷ and</p>	<p>Technical - agreed</p>

³³ OJ L 164, 22.6.2002, p. 3.

<p>offences as referred to in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States³⁴.</p>	<p>offences as referred to in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States³⁶.</p>	<p>of other serious criminal offences as referred to in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States³⁸.</p>	
<p>(25) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and shall be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying</p>	<p>(25) Requests for comparison with data stored in the EURODAC central database <i>should</i> be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and <i>should</i> be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data <i>should</i> not act as a verifying authority. The verifying</p>	<p>(25) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and shall be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying</p>	<p>EP suggestion to replace "shall" by "should" is accepted.</p> <p>EP suggestion to replace "shall" by "should" is accepted.</p>

³⁴ OJ L 190, 18.7.2002, p. 1.

³⁵ OJ L 164, 22.6.2002, p. 3.

³⁶ OJ L 190, 18.7.2002, p. 1.

³⁷ OJ L 164, 22.6.2002, p. 3.

³⁸ OJ L 190, 18.7.2002, p. 1.

<p>authorities should be responsible for ensuring strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.</p>	<p>authorities should be <i>independent of the designated authorities</i> and responsible for ensuring strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.</p>	<p>authorities should be responsible for ensuring <u>in an independent manner,</u> strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request <u>without forwarding the reasons for it,</u> for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency <u>where</u> early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.</p>	<p>Pres suggests to reword the sentence to the effect that "The verifying authorities should act independently of the designated authorities and should be responsible for ensuring in an independent manner, strict conditions... ". EP accepted this suggestion.</p> <p>EP accepts the Council amendment</p>
---	--	---	---

	(25a) <i>The designated authority and the verifying authority may be part of the same organisation if so stipulated under national law, but the verifying authority should have independence within the institutional structure.</i>		The Pres compromise suggestion is agreed and reads as follows: "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".
(26) 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 on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated	(26) 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 on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State, [...] with the Automated	(26) 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 on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated	As a result of the third informal trilogue a compromise has been provisionally agreed upon for this Recital by EP and Pres (<i>it is suggested to break the Recital up in three separate ones – 26, 26a and 26b for better drafting purposes</i>): Recital 26 will read: (26) 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 <i>in specific cases</i> and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious

<p>Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime³⁹ have returned negative results. This condition requires prior implementation of the Council Decision as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. 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 or other serious criminal offence, or to specific persons in respect of</p>	<p>Fingerprint Databases of other Member States under the 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 have returned negative results. This condition requires prior implementation of [...] Council Decision 2008/615/JHA as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. <i>Designated authorities should also, when possible, consult the Visa Information System under Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System</i></p>	<p>Fingerprint Databases of other Member States under the 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. This condition requires the Member State to conduct a comparison with the Automated Fingerprint Database of another Member State under Council Decision 2008/615/JHA and all further comparisons with other Member States under the Council Decision that are necessary and technically available. The comparison with the Automated Fingerprint Databases of [...] </p>	<p>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 or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist 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 or other serious criminal offence.</p> <p>This compromise suggestion is</p>
---	--	---	--

³⁹ OJ L 210, 6.8.2008, p. 1.

<p>whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist 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 or other serious criminal offence.</p>	<p><i>(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 offences⁴⁰ prior to consulting EURODAC.</i> 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 or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected</p>	<p><u>another Member State is not necessary in a specific case if there are no reasonable grounds to consider that this comparison will contribute to the prevention, detection or investigation of any of the criminal offences in question</u> ⁴¹. This condition requires prior ⁴¹ <u>legal and technical</u> ⁴¹ implementation of the Council Decision ⁴¹ <u>by the Member State in the area of fingerprint data,</u> ⁴¹ as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. A specific case exists in particular when the request for comparison is connected to a specific and concrete</p>	<p>provisionally agreed</p>
--	--	---	-----------------------------

⁴⁰ OJ L 218, 13.8.2008, p. 129.

⁴¹ OJ L 210, 6.8.2008, p. 1.

	<p>to a person who is a victim of a terrorist 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 or other serious criminal offence.</p>	<p>danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist 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 or other serious criminal offence.</p>	
--	--	---	--

			<p>On the basis of the tentative compromise reached for Recitals 26, 26a and 26b, Recital 26a will read as follows:</p> <p>In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime⁴² did not lead to the establishment of the identity of the data subject. This condition requires the Member State to conduct comparisons with the Automated Fingerprint Databases of all other Member States under Council Decision 2008/615/JHA which are technically available, unless they 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</p>
--	--	--	--

⁴² OJ L 210, 6.8.2008, p. 1.

			<p>reasonable grounds exist in particular where the specific case does not present any operational or investigatory link to a given Member State. This condition requires prior legal and technical implementation of the Council Decision by the Member State in the area of fingerprint data, as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken.</p> <p>This compromise on Recital 26a is provisionally agreed</p>
			<p>On the basis of the tentative compromise reached for Recitals 26, 26a and 26b, Recital 26b will read as follows:</p> <p>(26b) Designated authorities should also, provided that the conditions for such 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</p>

			designated authorities of Member States and by Europol for the purposes of the prevention, detection or investigation of terrorist offences and of other serious criminal offences ⁴³ prior to consulting EURODAC. This compromise on Recital 26b is dependent on the outcome of Art. 20(1) negotiations
	(26a) <i>For the purpose of efficient comparison and exchange of personal data, the 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 Council Decision 2008/615/JHA.</i>		This EP amendment will now be renumbered as draft Recital 26c. EP amendment is provisionally agreed.
(27) In case the requesting Member State establishes that EURODAC data pertains to a minor, these	(27) In case the requesting Member State establishes that EURODAC data pertains to a minor, these	(27) In case the requesting Member State establishes that EURODAC data pertains to a minor, these	Pres suggests the following compromise text which is due to replace the relevant EP amendments in Art. 3(5) and

⁴³ OJ L 218, 13.8.2008, p. 129.

<p>data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws for minors and in accordance with the obligation to give primary consideration to the child's best interest.</p>	<p>data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws for minors and in accordance with the obligation to give primary consideration to the child's best interest.</p>	<p>data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws for minors and in accordance with the obligation to give primary consideration to the child's best interest.</p>	<p>29(1)(e) in relation to the best interest of the child consideration:</p> <p>27) <i>The best interests of the child should be a primary consideration for the Member States when applying this Regulation. For law enforcement purposes, in case the requesting Member State establishes that EURODAC data pertains 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 for minors and in accordance with the obligation to give primary consideration to the child's best interest.</i></p>
<p>(28) While the non-contractual liability of the Community in connection with the operation of the EurodacEURODAC system will be governed by the relevant provisions of the Treaty, it is necessary to lay down specific rules for the non-contractual liability of the Member States in connection with the</p>	<p>(28) While the non-contractual liability of the Union in connection with the operation of the EurodacEURODAC system will be governed by the relevant provisions of the Treaty, 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.</p>	<p>(28) While the non-contractual liability of the [...] Union in connection with the operation of the EurodacEURODAC system will be governed by the relevant provisions of the Treaty, it is necessary to lay down specific rules for the non-contractual liability of the Member States in connection with the</p>	<p>Identical</p>

operation of the system.		operation of the system.	
<p>(29) In accordance with the principle of subsidiarity as set out in Article 5 of the Treaty, the objective of the proposed measures, namely the creation within the Commission of a system for the comparison of fingerprint data to assist the implementation of the Community's asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved by the Community. In accordance with the principle of proportionality as set out in the said Article, this Regulation does not go beyond what is necessary to achieve that <u>those</u> objectives.</p>	<p>(29) <i>Since the objective of this Regulation, namely the creation of a system for the comparison of fingerprint data to assist the implementation of the Union asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. 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.</i></p>	<p>(29) In accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on the European Union the , the objective of the proposed measures, namely the creation within the Commission of a system for the comparison of fingerprint data to assist the implementation of the the Union's asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved by the the Union . In accordance with the principle of proportionality as set out in the said Article, this Regulation does not go beyond what is necessary to achieve that <u>those</u> objectives.</p>	<p>Technical - the EP amendment agreed, based on the standard language on subsidiarity</p>

<p>(30) 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 data⁴⁴ applies to the processing of personal data by the Member States</p> <p>☒ carried out in application of this Regulation ☒ within the framework of the Eurodac system → unless such processing takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences ⇐.</p>	<p>(30) 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 data⁴⁵ applies to the processing of personal data by the Member States</p> <p>☒ carried out in application of this Regulation ☒ within the framework of the Eurodac system → unless such processing takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences ⇐.</p>	<p>(30) 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 data⁴⁶ applies to the processing of personal data by the Member States</p> <p>☒ carried out in application of this Regulation ☒ within the framework of the Eurodac system → unless such processing takes place by Member States' ☒ [...] authorities for the purposes of the prevention, detection and investigation of terrorist offences and ☒ of other serious criminal offences ⇐.</p>	<p>EP compromise, "designated or verifying authorities" is agreed .</p> <p>Council agreed to replace the "and" in the Council text by "or" and the "of" by "or of"</p>
<p>(31) Council Framework Decision 2008/977/JHA</p>	<p>(31) Council Framework Decision 2008/977/JHA</p>	<p>(31) ☒ [...] ☒ The processing of personal</p>	<p>EP to confirm agreement on the Council amendment; Council</p>

⁴⁴ OJ L 281, 23.11.1995, p. 31.

⁴⁵ OJ L 281, 23.11.1995, p. 31.

⁴⁶ OJ L 281, 23.11.1995, p. 31.

<p>of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters⁴⁷ applies to all processing of personal data by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.</p>	<p>of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters⁴⁸ applies to all processing of personal data by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.</p>	<p>data by Member States' of [...] of authorities for the purposes of the prevention, detection and investigation of terrorist offences and 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 is in line with Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. of .</p>	<p>agreed to replace the "and" at the Council text by "or" and the "of" by "or of"</p>
<p>(16) By virtue of Article 286 of the Treaty, Directive 95/46/EC also applies to Community institutions and bodies. Since the Central Unit will be established within the Commission, that</p>	<p>(16) By virtue of Article 286 of the Treaty, Directive 95/46/EC also applies to Community institutions and bodies. Since the Central Unit will be established within the Commission, that</p>	<p>(16) By virtue of Article 286 of the Treaty, Directive 95/46/EC also applies to Community institutions and bodies. Since the Central Unit will be established within the Commission, that</p>	

⁴⁷ OJ L 350, 30.12.2008, p. 60.

⁴⁸ OJ L 350, 30.12.2008, p. 60.

<p>Directive will apply to the processing of personal data by that Unit.</p>	<p>Directive will apply to the processing of personal data by that Unit.</p>	<p>Directive will apply to the processing of personal data by that Unit.</p>	
<p>(32) The principles set out in Directive 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data should be supplemented or clarified, in particular as far as certain sectors are concerned.</p>	<p>(32) The principles set out in Directive 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data should be supplemented or clarified, in particular as far as certain sectors are concerned.</p>	<p>(32) The principles set out in Directive 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data should be supplemented or clarified, in particular as far as certain sectors are concerned.</p>	<p>Identical</p>
<p>(33) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third</p>	<p>(33) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third</p>	<p>(33) Transfers of data obtained pursuant to this Decision [...] Decision Regulation to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data</p>	<p>As a result of the third informal trilogue EP and Pres agreed to test the following wording:</p> <p>Transfers of data obtained pursuant to this Regulation to third countries or international organisations or private entities, as well as such data subsequently further processed at national level, should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international</p>

<p>country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.</p>	<p>country. <i>The prohibition of transfer to third countries should cover both EURODAC data obtained under this Regulation and personal data exchanged bilaterally subsequent to a EURODAC search which are stored or processed at national level.</i> This prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]* applies, in order to ensure that Member States have the possibility of</p>	<p>disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.</p>	<p>protection from having their data disclosed to any third country. This implies that Member States can under no circumstances transfer information obtained from the Eurodac central system concerning the Member State(s) of origin, place and date of the application for international protection, the status of the person as well as the date of arrival, departure or removal from the territory of the Member States or the date when the decision to examine the application for international protection was taken, his or her fingerprints and the date on which they were taken, his or her sex as well as the date on which the Member State(s) transmitted the data to Eurodac. This prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for</p>
---	---	--	--

	<p>cooperating with such third countries for the purposes of this Regulation. <i>That right should not apply to transfers of data to third countries in the context of law enforcement.</i></p>		<p>examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]* applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.</p> <p>The Pres suggests the following alternative compromise wording:</p> <p>Transfers of Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC Central System to any third country or international organisation or a private entity established in or outside the European Union, as well as such data subsequently further processed at national level, should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This implies that Member States cannot under no circumstances transfer</p>
--	---	--	--

			<p>information obtained from the Eurodae EURODAC eCentral sSystem concerning: the Member State(s) of origin; place and date of the application for international protection; the status of the person as well as the date of arrival, departure or removal from the territory of the Member States or the date when the decision to examine the application for international protection was taken, his or her fingerprints and the date on which they were taken, his or her sex, 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 Eurodae EURODAC; the operator user ID; and any information relating to any transfer of the data subject under the Dublin Regulation.</p> <p>This prohibition should be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an</p>
--	--	--	---

			<p>application for international protection lodged in one of the Member States by a third-country national or a stateless person]* applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.</p> <p>The Pres recommends acceptance of its alternative wording, with regard to working out an overall compromise.</p>
			<p>As a result of the third informal trilogue a new Recital 33a is suggested to be added:</p> <p>(33a) Personal data obtained from another Member State further to a hit in Eurodac should only be transferred to a third country pursuant to Council Framework Decision 2008/977/JHA according to which such transfer should, in principle, take place only after the Member State from which the data were</p>

			<p>obtained has given its consent to the transfer. Any transfer of personal data to a third country should be prohibited if there is a serious risk of the data subject being subjected to torture, inhuman and degrading treatment or punishment or any other violation of fundamental rights.</p> <p>The Pres recommends deletion of this draft Recital, as the concept is already covered by Art. 35.</p>
<p>(34) National competent authorities for the supervision of the processing of personal data should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by the Europol Decision should monitor the lawfulness of data processing activities</p>	<p>(34) National competent authorities for the supervision of the processing of personal data should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by the Europol Decision should monitor the lawfulness of data processing activities</p>	<p>(34) National ... supervisory authorities ... should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by the Europol Decision should monitor the lawfulness of data processing activities</p>	<p>Council amendment agreed</p>

performed by Europol.	performed by Europol.	performed by Europol.	
<p>(35) 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 data⁴⁹ and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply 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.</p>	<p>(35) 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 <i>Union</i> institutions and bodies and on the free movement of such data and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply 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, <i>bearing in mind that data protection is a key factor in the</i></p>	<p>(35) 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 data⁵⁰ and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply 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.</p>	<p>Technical - agreed</p> <p>EP amendment agreed.</p>

	<p><i>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 [.../...] [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]*.</i></p>		
	<p>(35a) <i>The data subject should be informed of the purpose for which his or her data will be processed within EURODAC, including a description of the aims of Regulation (EU) No</i></p>		EP amendment agreed.

	<i>[.../...] [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 the use to which law enforcement authorities may put his or her data.</i>		
(36) 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 Article 41 of 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	(36) 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 Article 41 of 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	(36) 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 Article 41 of 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	Identical

out in application of this Regulation.	out in application of this Regulation.	out in application of this Regulation.	
(37) It is appropriate to monitor and evaluate the performance of Eurodac EURODAC ⇨ at regular intervals ⇩.	(37) It is appropriate to monitor and evaluate the performance of EURODAC at regular intervals, <i>including in terms of whether law enforcement access has led to the stigmatisation of applicants for international protection as raised in the Commission's evaluation of the compliance of the proposal with the Charter of Fundamental Rights. The Agency should submit an annual report on the activities of the Central System to the European Parliament and to the Council.</i>	(37) It is appropriate to monitor and evaluate the performance of Eurodac EURODAC ⇨ at regular intervals ⇩.	EP compromise on its amendment: replace "stigmatisation" by indirect discrimination" EP amendment, with the compromise is accepted.
(38) Member States should provide for a system of effective effective, proportionate and dissuasive dissuasive penalties to sanction the processing use processing use of data entered in the central database central database	(38) Member States should provide for a system of effective effective, proportionate and dissuasive dissuasive penalties to sanction the processing use processing use of data entered in the central database central database	(38) Member States should provide for a system of effective effective, proportionate and dissuasive dissuasive penalties to sanction the processing use processing use of data entered in the central database central database	Identical

<p>⇒ Central System ⇐ contrary to the purpose of EurodacEURODAC.</p>	<p>⇒ Central System ⇐ contrary to the purpose of EurodacEURODAC.</p>	<p>⇒ Central System ⇐ contrary to the purpose of EurodacEURODAC.</p>	
<p>(39) It is necessary that Member States are informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].</p>	<p>(39) It is necessary that Member States <i>be</i> informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*.</p>	<p>(39) It is necessary that Member States are informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].</p>	<p>Identical</p>
<p>(40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In</p>	<p>(40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In</p>	<p>(40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In</p>	<p>The Pres recommends acceptance of the EP amendment</p>

<p>particular, this Regulation fully respects the individual's right to protection of his or her personal data and the right to asylum.</p>	<p>particular, this Regulation <i>seeks to ensure full respect for the</i> protection of personal data and the right to <i>seek</i> asylum <i>and to promote the application of Articles 8 and 18 of the Charter.</i></p>	<p>particular, this Regulation fully respects the individual's right to protection of his or her personal data and the right to asylum.</p>	
<p>(41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. As regards Denmark, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes amendment to the EURODAC</p>	<p>(41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. As regards Denmark, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes amendment to the EURODAC</p>	<p>(41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. As regards Denmark, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes amendment to the EURODAC</p>	<p>Identical</p>

<p>Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention⁵¹. Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union. Once this Recast Regulation is</p>	<p>Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention⁵². Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union. Once this Recast Regulation is</p>	<p>Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention⁵³. Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union. Once this Recast Regulation is</p>	
---	---	---	--

<p>adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, Denmark will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.</p>	<p>adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, Denmark will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.</p>	<p>adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, Denmark will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.</p>	
<p>(42) In accordance with Article 3 of the Protocol 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 <i>is</i></p>	<p>(42) In accordance with Article 3 of the Protocol 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 <i>is</i></p>	<p>(42) In accordance with Article 3 of the Protocol 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 <i>is</i></p>	<p>Identical</p>

<p><i>not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation].</i></p>	<p><i>not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation].</i></p>	<p><i>not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation].</i></p>	
<p>(43) In accordance with Article 3 of the Protocol 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 <i>[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation].</i></p>	<p>(43) In accordance with Article 3 of the Protocol 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 <i>[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation].</i></p>	<p>(43) In accordance with Article 3 of the Protocol 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 <i>[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation].</i></p>	<p>Identical</p>

<p>(44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway⁵⁴. Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be</p>	<p>(44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway⁵⁵. Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be</p>	<p>(44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway⁵⁶. Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be</p>	<p>Identical</p>
--	--	--	------------------

<p>applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in there relations with the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Republic of Iceland and the Kingdom of Norway will be consulted as to whether they wish to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.</p>	<p>applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in there relations with the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Republic of Iceland and the Kingdom of Norway will be consulted as to whether they wish to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.</p>	<p>applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in there relations with the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Republic of Iceland and the Kingdom of Norway will be consulted as to whether they wish to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.</p>	
<p>(45) As regards the Swiss Confederation, this Regulation, with the exception of the</p>	<p>(45) As regards the Swiss Confederation, this Regulation, with the exception of the</p>	<p>(45) As regards the Swiss Confederation, this Regulation, with the exception of the</p>	<p>Identical</p>

<p>procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland⁵⁷. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission</p>	<p>procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland⁵⁸. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission</p>	<p>procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland⁵⁹. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission</p>	
--	--	--	--

<p>recommendation for a Council Decision authorising the opening of negotiations, the Swiss Confederation will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on the application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.</p>	<p>recommendation for a Council Decision authorising the opening of negotiations, the Swiss Confederation will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on the application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.</p>	<p>recommendation for a Council Decision authorising the opening of negotiations, the Swiss Confederation will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on the application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.</p>	
<p>(46) As regards the Principality of Liechtenstein, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in</p>	<p>(46) As regards the Principality of Liechtenstein, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in</p>	<p>(46) As regards the Principality of Liechtenstein, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in</p>	<p>Identical</p>

<p>Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland⁶⁰. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss</p>	<p>Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland⁶¹. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss</p>	<p>Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland⁶². Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss</p>	
--	--	--	--

<p>Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Principality of Liechtenstein will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on their application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.</p>	<p>Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Principality of Liechtenstein will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on their application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.</p>	<p>Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Principality of Liechtenstein will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on their application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.</p>	
---	---	---	--

<p>(47) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of the Dublin Convention</p> <p>☒ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ☒ .</p>	<p>(47) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of the Dublin Convention</p> <p>☒ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ☒ .</p>	<p>(47) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of the Dublin Convention</p> <p>☒ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ☒ .</p>	<p>Identical</p>
<p>HAVE ADOPTED THIS REGULATION:</p>	<p>HAVE ADOPTED THIS REGULATION:</p>	<p>HAVE ADOPTED THIS REGULATION:</p>	

CHAPTER I	CHAPTER I	CHAPTER I	
GENERAL PROVISIONS	GENERAL PROVISIONS	GENERAL PROVISIONS	
<i>Article 1</i> Purpose of "EurodacEURODAC"	<i>Article 1</i> Purpose of "EurodacEURODAC"	<i>Article 1</i> Purpose of "EurodacEURODAC"	
1. A system known as " Eurodac EURODAC" is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to the Dublin Convention <input checked="" type="checkbox"/> Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>	1. A system known as " Eurodac EURODAC" is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to the Dublin Convention <input checked="" type="checkbox"/> Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>	1. A system known as " Eurodac EURODAC" is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to the Dublin Convention <input checked="" type="checkbox"/> Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>	Identical

<p>for examining an application for asylum ⇒ international protection ⇐ lodged in a Member State ⇒ by a third country national or a stateless person ⇐, and otherwise to facilitate the application of the Dublin Convention ⊗ Regulation ⊗ under the conditions set out in this Regulation.</p>	<p>for examining an application for asylum ⇒ international protection ⇐ lodged in a Member State ⇒ by a third country national or a stateless person ⇐, and otherwise to facilitate the application of the Dublin Convention ⊗ Regulation ⊗ under the conditions set out in this Regulation.</p>	<p>for examining an application for asylum ⇒ international protection ⇐ lodged in a Member State ⇒ by a third country national or a stateless person ⇐, and otherwise to facilitate the application of the Dublin Convention ⊗ Regulation ⊗ under the conditions set out in this Regulation.</p>	
2. Eurodac shall consist of:	2. Eurodac shall consist of:	2. Eurodac shall consist of:	
(a) the Central Unit referred to in Article 3;	(a) the Central Unit referred to in Article 3;	(a) the Central Unit referred to in Article 3;	
(b) a computerised central database in which the data referred to in Article 5(1), Article 8(2) and Article 11(2) are processed for the purpose of comparing the fingerprint data of applicants for asylum and of the categories of aliens referred to in Article 8(1) and Article 11(1);	(b) a computerised central database in which the data referred to in Article 5(1), Article 8(2) and Article 11(2) are processed for the purpose of comparing the fingerprint data of applicants for asylum and of the categories of aliens referred to in Article 8(1) and Article 11(1);	(b) a computerised central database in which the data referred to in Article 5(1), Article 8(2) and Article 11(2) are processed for the purpose of comparing the fingerprint data of applicants for asylum and of the categories of aliens referred to in Article 8(1) and Article 11(1);	
(c) means of data	(c) means of data	(c) means of data transmission	

<p>transmission between the Member States and the central database.</p>	<p>transmission between the Member States and the central database.</p>	<p>between the Member States and the central database.</p>	
<p>2. This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.</p>	<p>2. This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.</p>	<p>2. This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and of <u>of</u> other serious criminal offences of <u>("law enforcement purposes")</u>.</p>	<p>Technical amendment - agreed</p>

<p>3. Without prejudice to the <u>processing use</u> of data intended for EurodacEURODAC 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 EurodacEURODAC only for the purposes set out in ⇒ this Regulation and ⇐ Article 15(1)32(1) of the Dublin Convention ⇒ this Regulation and ⇐ Article 15(1)32(1) of the Dublin Convention ⊗ Regulation ⊗ .</p>	<p>3. Without prejudice to the <u>processing use</u> of data intended for EurodacEURODAC 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 EurodacEURODAC only for the purposes set out in ⇒ this Regulation and ⇐ Article 15(1)32(1) of the Dublin Convention ⇒ this Regulation and ⇐ Article 15(1)32(1) of the Dublin Convention ⊗ Regulation ⊗ .</p>	<p>3. Without prejudice to the <u>processing use</u> of data intended for EurodacEURODAC 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 EurodacEURODAC only for the purposes set out in ⇒ this Regulation and ⇐ Article 15(1)32(1) of the Dublin Convention ⇒ this Regulation and ⇐ Article 15(1)32(1) of the Dublin Convention ⊗ Regulation ⊗ .</p>	<p>Identical</p> <p>Technical - reference should be made to Art. 34 of the Dublin Regulation</p>
<p><i>Article 2</i> Definitions</p>	<p><i>Article 2</i> Definitions</p>	<p><i>Article 2</i> Definitions</p>	
<p>1. For the purposes of this Regulation:</p>	<p>1. For the purposes of this Regulation:</p>	<p>1. For the purposes of this Regulation:</p>	
<p>(a) "the Dublin Convention ⊗ Regulation ⊗ " means the Convention determining the State responsible for examining</p>	<p>(a) "the Dublin Convention ⊗ Regulation ⊗ " means the Convention determining the State responsible for examining</p>	<p>(a) "the Dublin Convention ⊗ Regulation ⊗ " means the Convention determining the State responsible for examining</p>	<p>Identical</p>

<p>applications for asylum lodged in one of the Member States of the European Communities, signed at Dublin on 15 June 1990</p> <p><input checked="" type="checkbox"/> Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>.</p>	<p>applications for asylum lodged in one of the Member States of the European Communities, signed at Dublin on 15 June 1990</p> <p><input checked="" type="checkbox"/> Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>.</p>	<p>applications for asylum lodged in one of the Member States of the European Communities, signed at Dublin on 15 June 1990</p> <p><input checked="" type="checkbox"/> Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] <input checked="" type="checkbox"/>.</p>	
<p>(b) an "applicant for asylum ⇒ international protection ⇐" means an alien <input checked="" type="checkbox"/> third-country national or a</p>	<p>(b) an "applicant for asylum ⇒ international protection ⇐" means an alien <input checked="" type="checkbox"/> third-country national or a</p>	<p>(b) an "applicant for asylum ⇒ international protection ⇐" means an alien <input checked="" type="checkbox"/> third-country national or a</p>	

<p>stateless person ☒ who has made an application for asylum or on whose behalf such an application has been made ⇒ international protection as defined in Article 2(g) of Council Directive 2004/83/EC in respect of which a final decision has not yet been taken ⇐;</p>	<p>stateless person ☒ who has made an application for asylum or on whose behalf such an application has been made ⇒ international protection as defined in Article 2(g) of Council Directive 2004/83/EC in respect of which a final decision has not yet been taken ⇐;</p>	<p>stateless person ☒ who has made an application for asylum or on whose behalf such an application has been made ⇒ international protection as defined in Article 2(g) of Council Directive 2004/83/EC in respect of which a final decision has not yet been taken ⇐;</p>	<p>Reference should be made to the new Qualification Directive (Directive 2011/95/EU)</p>
<p>(c) "Member State of origin" means:</p>	<p>(c) "Member State of origin" means:</p>	<p>(c) "Member State of origin" means:</p>	
<p>(i) in relation to an applicant for asylum ☒ person covered by Article 6 ☒, the Member State which transmits the personal data to the Central Unit</p>	<p>(i) in relation to an applicant for asylum ☒ person covered by Article 6 ☒, the Member State which transmits the personal data to the Central Unit</p>	<p>(i) in relation to an applicant for asylum ☒ person covered by Article 9 ☐ ☐ [...] ☐ ☒, the Member State which transmits the personal data</p>	<p>Technical - agreed</p>

<p>⇒ System ⇐ and receives the results of the comparison;</p>	<p>⇒ System ⇐ and receives the results of the comparison;</p>	<p>to the Central Unit ⇒ System ⇐ and receives the results of the comparison;</p>	
<p>(ii) in relation to a person covered by Article 8 <u>11</u> , the Member State which transmits the personal data to the Central Unit ⇒ System ⇐;</p>	<p>(ii) in relation to a person covered by Article 8 <u>11</u> , the Member State which transmits the personal data to the Central Unit ⇒ System ⇐;</p>	<p>(ii) in relation to a person covered by Article 8 ⇒ [...] ⇐ ⇒ <u>14</u> ⇐ , the Member State which transmits the personal data to the Central Unit ⇒ System ⇐;</p>	<p>Technical - agreed</p>
<p>(iii) in relation to a person covered by Article 11 <u>14</u> , the Member State which transmits such data to the Central Unit ⇒ System ⇐</p>	<p>(iii) in relation to a person covered by Article 11 <u>14</u> , the Member State which transmits such data to the Central Unit ⇒ System ⇐</p>	<p>(iii) in relation to a person covered by Article 11 ⇒ [...] ⇐ ⇒ <u>17</u> ⇐ , the Member State which transmits such data to the Central</p>	<p>Technical - agreed</p>

<p>and receives the results of the comparison;</p>	<p>and receives the results of the comparison;</p>	<p>Unit ⇒ System ⇐ and receives the results of the comparison;</p>	
<p>(d) "refugee" ⇒ "person granted international protection" ⇐ means a ☒ third country national or a stateless ☒ person who has been recognised as a refugee in accordance with the Geneva Convention on Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967 ⇒ entitled to international protection as defined in point (a) of Article 2 of Council Directive 2004/83/EC ⇐;</p>	<p>(d) <i>"beneficiary of international protection"</i> means a third country national or a stateless person <i>who has been granted international protection as defined in Article 2(a) of Directive 2011/95/EU;</i></p>	<p>(d) "refugee" ⇒ "person granted international protection" ⇐ means a ☒ third country national or a stateless ☒ person who has been recognised as a refugee in accordance with the Geneva Convention on Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967 ⇒ entitled to international protection as defined in point (a) of Article 2 of Council Directive 2004/83/EC ⇐;</p>	<p>Technical - agreed</p>

<p>(e) "hit" shall mean the existence of a match or matches established by the Central Unit ⇒ System ⇐ by comparison between fingerprint data recorded in the databank ☒ 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 4(6) 18(4);</p>	<p>(e) "hit" <i>means</i> the existence of a match or matches established by the Central System by comparison between fingerprint data recorded in the <i>computerised</i> 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 18(4);</p>	<p>(e) "hit" shall mean the existence of a match or matches established by the Central Unit ⇒ System ⇐ by comparison between fingerprint data recorded in the databank ☒ 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 4(6) ⇒ [...] ⇐ ⇒ 25 ⇐ (4);</p>	<p>Technical amendment - EP text agreed</p> <p>Technical - EP amendment agreed</p> <p>Technical - Council amendment agreed</p>
<p>(f) "National Access Point" means the designated national system which communicates with the Central</p>	<p>(f) "National Access Point" means the designated national system which communicates with the Central</p>	<p>(f) "National ⇒ [...] ⇐ ⇒ Access ⇐ Point" means the designated national system which communicates with the Central</p>	<p>Technical - Council text agreed</p>

System;	System;	System;	
(g) "Agency" means the Agency established by Regulation (EU) No 1077/2011;	(g) "Agency" means the Agency established by Regulation (EU) No 1077/2011;	(g) "Agency" means the Agency established by Regulation (EU) No 1077/2011;	Identical
(h) 'Europol' means the European Police Office as established by Decision 2009/371/JHA;	(h) 'Europol' means the European Police Office as established by Decision 2009/371/JHA;	(h) 'Europol' means the European Police Office as established by Decision 2009/371/JHA;	Identical
(i) 'EURODAC data' means all fingerprint data stored in the central database in accordance with Article 11 and Article 16(2);	(i) 'EURODAC data' means all fingerprint data stored in the central database in accordance with Article 11 and Article 16(2);	(i) 'EURODAC data' means all [...] data stored in the central database in accordance with Article 11 and Article [...] 14 (2);	Council text agreed
(j) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of Framework	(j) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of Framework	(j) 'terrorist - related offences' means the offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of	the Cion originally proposed text is provisionally agreed

Decision 2002/475/JHA;	Decision 2002/475/JHA;	Framework Decision 2002/475/JHA;	
(k) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law;	(k) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law;	(k) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law;	Identical
(l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent.	(l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent.	(l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent.	Identical

<p>personal data are processed by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.</p>	<p>personal data are processed by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.</p>	<p>personal data are processed by Member States' ... authorities for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences pursuant to this Regulation.</p>	<p>be made to all authorities involved, i.e. also to the verifying authorities and the national contact points, for clarification purposes</p> <p>Council agreed to replace the "and" at the Council text by "or" and the "of" by "or of"</p>
<p><i>Article 3</i> Central Unit <input checked="" type="checkbox"/> System architecture and basic principles <input checked="" type="checkbox"/></p>	<p><i>Article 3</i> Central Unit <input checked="" type="checkbox"/> System architecture and basic principles <input checked="" type="checkbox"/></p>	<p><i>Article 3</i> Central Unit <input checked="" type="checkbox"/> System architecture and basic principles <input checked="" type="checkbox"/></p>	
<p>1. A Central Unit shall be established within the Commission which shall be responsible for operating the central database referred to in Article 1(2)(b) on behalf of the Member States. The Central Unit shall be equipped with a computerised fingerprint recognition system.</p>	<p>1. A Central Unit shall be established within the Commission which shall be responsible for operating the central database referred to in Article 1(2)(b) on behalf of the Member States. The Central Unit shall be equipped with a computerised fingerprint recognition system.</p>	<p>1. A Central Unit shall be established within the Commission which shall be responsible for operating the central database referred to in Article 1(2)(b) on behalf of the Member States. The Central Unit shall be equipped with a computerised fingerprint recognition system.</p>	
<p>1. EURODAC shall consist of:</p>	<p>1. EURODAC shall consist of:</p>	<p>1. EURODAC shall consist of:</p>	

(a) a computerised central fingerprint database (Central System) composed of	(a) a computerised central fingerprint database (Central System) composed of:	(a) a computerised central fingerprint database (Central System) composed of	Identical
– a Central Unit,	– a Central Unit,	– a Central Unit,	
– a Business Continuity System.	– a Business Continuity <i>Plan</i> .	– a Business Continuity System.	The Council and EP could agreed on a compromise based on a combination of the two amendments: "a Business Continuity Plan and System"
(b) a communication infrastructure between the Central System and Member States that provides an encrypted virtual network dedicated to EURODAC data (Communication Infrastructure).	(b) a communication infrastructure between the Central System and Member States that provides an encrypted virtual network dedicated to EURODAC data (Communication Infrastructure).	(b) a communication infrastructure between the Central System and Member States that provides an encrypted virtual network dedicated to EURODAC data (Communication Infrastructure).	Identical
2. Each Member State shall have a single National Access Point.	2. Each Member State shall have a single National Access Point.	2. Each Member State shall have a single National Access Point.	Identical
2.3. Data on applicants for asylum , persons covered by Articles 8 and persons	2.3. Data on applicants for asylum , persons covered by Articles 8 and persons	2.3. Data on applicants for asylum , persons covered by Articles 8 and persons	Identical

<p>covered by Article 11 9, 14 and 17 which are processed in the Central Unit ⇒ 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>covered by Article 11 9, 14 and 17 which are processed in the Central Unit ⇒ 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>covered by Article 11 9, 14 and 17 which are processed in the Central Unit ⇒ 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><u>4.</u> The rules governing EurodacEURODAC shall also apply to operations effected by the Member States as from the transmission of data to the Central Unit ⇒ System ⇐ until use is made of the results of the comparison.</p>	<p><u>4.</u> The rules governing EurodacEURODAC shall also apply to operations effected by the Member States as from the transmission of data to the Central Unit ⇒ System ⇐ until use is made of the results of the comparison.</p>	<p><u>4.</u> The rules governing EurodacEURODAC shall also apply to operations effected by the Member States as from the transmission of data to the Central Unit ⇒ System ⇐ until use is made of the results of the comparison.</p>	Identical
<p><u>5.</u> The procedure for taking fingerprints shall be determined ⇒ and applied ⇐ in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in ⇒ the Charter of</p>	<p><u>5.</u> The procedure for taking fingerprints shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of</p>	<p><u>5.</u> The procedure for taking fingerprints shall be determined ⇒ and applied ⇐ in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in ⇒ the Charter of</p>	

<p>Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and the European Convention on Human Rights and in the United Nations Convention on the Rights of the Child.</p>	<p>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>The best interests of the child shall be a primary consideration for the Member States when applying this Regulation.</i></p>	<p>Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and the European Convention on Human Rights and in the United Nations Convention on the Rights of the Child.</p>	<p>EP have agreed to the deletion of the word "primary" but insists on maintaining a provision in the operative part of the Regulation.</p> <p>The Pres recommends acceptance of the amended Recital 27, which would replace this provision.</p>
<p>Article 4 Operational management</p>	<p>Article 4 Operational management</p>	<p>Article 4 Operational management</p>	
<p>1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central System.</p>	<p>1. The Agency shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available <i>and most secure technology and techniques</i>, subject to a cost-benefit analysis, <i>are</i> used for the Central</p>	<p>1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central System.</p>	<p>Technical - EP amendment</p>

	System.		accepted
2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure:	2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure:	2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure:	Identical
(a) supervision;	(a) supervision;	(a) supervision;	
(b) security;	(b) security;	(b) security;	
(c) the coordination of relations between the Member States and the provider.	(c) the coordination of relations between the Member States and the provider.	(c) the coordination of relations between the Member States and the provider.	
3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:	3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:	3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:	Identical
(a) tasks relating to implementation of the budget;	(a) tasks relating to implementation of the budget;	(a) tasks relating to implementation of the budget;	
(b) acquisition and renewal;	(b) acquisition and renewal;	(b) acquisition and renewal;	
(c) contractual matters.	(c) contractual matters.	(c) contractual matters.	

<p>4. Before the Agency takes up its responsibilities, the Commission shall be responsible for all tasks attributed to the Agency by this Regulation.</p>	<p>4. Before the Agency takes up its responsibilities, the Commission shall be responsible for all tasks attributed to the Agency by this Regulation.</p>	<p>4. Before the Agency takes up its responsibilities, the Commission shall be responsible for all tasks attributed to the Agency by this Regulation.</p>	<p>Identical</p>
<p>5. Operational management of EURODAC shall consist of all the tasks necessary to keep EURODAC functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System.</p>	<p>5. Operational management of EURODAC shall consist of all the tasks necessary to keep EURODAC functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System. <i>A Business Continuity Plan shall be developed taking into account maintenance needs and unforeseen downtime of the system, including the impact of business</i></p>	<p>5. Operational management of EURODAC shall consist of all the tasks necessary to keep EURODAC functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System.</p>	<p>EP amendment accepted by the Council (see also Art. 3(1)(a) second indent)</p>

	<i>continuity measures on data protection and security.</i>		
6. Without prejudice to Article 17 of Regulation No 31 (EEC), 11 (EAEC) ⁶³ , the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with EURODAC data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.	6. Without prejudice to Article 17 of Regulation No 31 (EEC), 11 (EAEC) ⁶⁴ , the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with EURODAC data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.	6. Without prejudice to Article 17 of Regulation No 31 (EEC), 11 (EAEC) ⁶⁵ , the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with EURODAC data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.	Identical
Article 5 Designated Authorities for the purpose of law enforcement access	Article 5 Designated Authorities for the purpose of law enforcement access	Article 5 Designated Authorities for the purpose of law enforcement access	
1. Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this	1. <i>For the purposes laid down in Article 1(2)</i> , Member States shall designate the authorities which are authorised to	1. For the purposes as laid down in Article 1(2) Member States shall designate the authorities which are	EP linguistic remark (deletion of the word "as") agreed to be applied throughout the text

<p>Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.</p>	<p>access 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 and other serious criminal offences. Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security.</p>	<p>authorised to access EURODAC data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are [...] competent for the prevention, detection [...] and investigation of terrorist offences [...] or other serious criminal offences.</p>	<p>EP suggestion for maintaining the word "responsible", instead of "competent" is agreed.</p> <p>The EP additional text is agreed.</p>
<p>2. Every Member State shall keep a list of the designated authorities.</p>	<p>2. Every Member State shall keep a list of the designated authorities.</p>	<p>2. Every Member State shall keep a list of the designated authorities.</p>	<p>Identical</p>
<p>3. At national level, 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.</p>	<p>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.</p>	<p>3. At national level, 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.</p>	<p>Technical – agreed</p> <p>The word "operating" shall be replaced by "operational", in accordance with Art. 7(2).</p>

<p style="text-align: center;"><i>Article 6</i> Verifying Authorities</p>	<p style="text-align: center;"><i>Article 6</i> Verifying Authorities</p>	<p style="text-align: center;"><i>Article 6</i> Verifying Authorities <u>for the purposes of law enforcement access</u></p>	<p>Technical amendment - Council text agreed</p>
<p>1. Each Member State shall designate a single national body 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 and other serious criminal offences.</p>	<p>1. Each Member State shall designate a single national body 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 and other serious criminal offences, <i>shall act independently of the designated authorities referred to in Article 5 and shall not receive instructions from them as regards the outcome of the verification.</i></p>	<p>1. <u>For the purposes as laid down in Article 1(2) each</u> [...] <u>Member State shall designate a single national</u> [...] <u>authority or a branch of such an authority</u> to act as its verifying authority. The verifying authority shall be an authority of the Member State which is [...] <u>competent</u> for the prevention, detection [...] <u>or</u> investigation of terrorist offences [...] <u>or</u> other serious criminal offences.</p>	<p>Technical amendment - Council text agreed</p> <p>Council text is agreed with the change of the word "branch" to "unit".</p> <p>EP suggestion for maintaining the word "<u>responsible</u>", instead of "competent" is agreed.</p> <p>In relation to EP additional text, the Pres recommends the following compromise (including alignment with the agreed text of Recital 25a, whilst replacing "should" with "shall"):</p> <p>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</p>

			<p>its tasks under this Regulation. The verifying authority shall be separate from those units referred to in Article 5 and shall not receive instructions from them as regards the outcome of the verification.</p> <p>The Pres recommends acceptance of the above compromise.</p> <p>The Pres also recommends the acceptance of the following text:</p> <p>Member States may designate more than one verifying authority to reflect their organisational and administrative structures, in fulfilment of their constitutional or legal requirements.</p>
2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.	2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.	2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.	Identical
	<i>Only duly empowered staff of the verifying</i>		EP compromise text:

	<i>authority shall be authorised to access EURODAC in accordance with Article 19.</i>		<i>Only duly empowered staff of the verifying authority shall be authorised to <u>receive and transmit a request for access to EURODAC in accordance with Article 19</u></i> EP compromise is agreed
Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point which communicates with the Central System.	Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point which communicates with the Central System.	Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point which communicates with the Central System.	Identical
Article 7 Europol	Article 7 Europol	Article 7 Europol	
1. Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its	1. Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority, <i>which shall act independently of the designated authorities referred to in Article 5 and shall not receive instructions from them</i>	1. <u>☞ For the purposes as laid down in Article 1(2) ☞</u> Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority <u>☞</u> . <u>The verifying authority shall be a unit of Europol which acts independently.</u>	Technical amendment - Council text agreed EP compromise text, with further suggestions by the Pres (in bold/underline/italics), in order to align it with agreed language:

<p>requests for comparison of fingerprint data to the Central System.</p>	<p><i>as regards the outcome of the verification</i>, and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.</p>	<p>The unit shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled. Europol and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.</p>	<p>1. ☞ For the purposes as laid down in Article 1(2) ☞ Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority, <i>which shall act independently of the designated authority referred to in paragraph 2, when performing its tasks under this Regulation, and shall not receive instructions from the designated authority as regards the outcome of the verification.</i> The unit shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled. Europol and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.</p> <p>Compromise provisionally agreed.</p>
<p>2. Europol shall designate an operating unit that is authorised to request comparisons with EURODAC data through its designated National</p>	<p>2. Europol shall designate an operating unit that is authorised to request comparisons with EURODAC data through its designated National</p>	<p>2. Europol shall designate an operating unit that is authorised to request comparisons with EURODAC data through its designated National</p>	

<p>Access Point.</p>	<p>Access Point.</p>	<p>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 and investigating terrorist offences or other serious criminal offences falling under Europol's mandate. ➔</p>	<p>Council text agreed with the change of the word "operating" to "operational".</p>
<p>Article 8 3 ⊗ Statistics ⊗</p>	<p>Article 8 3 ⊗ Statistics ⊗</p>	<p>Article 8 3 ⊗ Statistics ⊗</p>	
<p>3=1. The Central Unit Agency ⊗ shall draw up statistics on its the ⊗ work ⊗ of the Central System ⊗ every quarter ⇒ month ⇐, indicating ⇒ in particular ⇐ :</p>	<p>1. The Agency shall draw up statistics on the work of the Central System every <i>quarter</i>, indicating in particular:</p>	<p>3=1. The Central Unit Agency ⊗ shall draw up statistics on its the ⊗ work ⊗ of the Central System ⊗ every quarter ⇒ month ⇐, indicating ⇒ in particular ⇐ :</p>	<p>EP amendment is agreed</p>
<p>(a) the number of data sets transmitted on persons referred to</p>	<p>(a) the number of data sets transmitted on persons referred to</p>	<p>(a) the number of data sets transmitted on applicants for</p>	<p>Identical</p>

<p>in Articles 9(1), 8(1) and 11(1) <u>14(1) and 17(1)</u> ;</p>	<p>in Articles 9(1), 8(1) and 11(1) <u>14(1) and 17(1)</u> ;</p>	<p>asylum and the persons referred to in Articles 9(1), 8(1) and 11(1) <u>14(1) and 17(1)</u> ;</p>	
<p>(b) the number of hits for applicants for asylum ⇒ international protection ⇐ who have lodged an application for asylum ⇒ international protection ⇐ in another Member State;</p>	<p>(b) the number of hits for applicants for asylum ⇒ international protection ⇐ who have lodged an application for asylum ⇒ international protection ⇐ in another Member State;</p>	<p>(b) the number of hits for applicants for asylum ⇒ international protection ⇐ who have lodged an application for asylum ⇒ international protection ⇐ in another Member State;</p>	<p>Identical</p>
<p>(c) the number of hits for persons referred to in Article 8(1) <u>14(1)</u> who have subsequently lodged an application for asylum ⇒ international protection ⇐;</p>	<p>(c) the number of hits for persons referred to in Article 8(1) <u>14(1)</u> who have subsequently lodged an application for asylum ⇒ international protection ⇐;</p>	<p>(c) the number of hits for persons referred to in Article 8(1) <u>14(1)</u> who have subsequently lodged an application for asylum ⇒ international protection ⇐;</p>	<p>Identical</p>
<p>(d) the number of hits for persons referred to in Article 11(1)</p>	<p>(d) the number of hits for persons referred to in Article 11(1)</p>	<p>(d) the number of hits for persons referred to in Article 11(1)</p>	<p>Identical</p>

<p><u>17(1)</u> who had previously lodged an application for asylum ⇒ international protection ⇐ in another Member State;</p>	<p><u>17(1)</u> who had previously lodged an application for asylum ⇒ international protection ⇐ in another Member State;</p>	<p><u>17(1)</u> who had previously lodged an application for asylum ⇒ international protection ⇐ in another Member State;</p>	
<p>(e) the number of fingerprint data which the Central Unit ⇒ System ⇐ had to ⇒ repeatedly ⇐ request a second time from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;<u>;</u></p>	<p>(e) the number of fingerprint data which the Central Unit ⇒ System ⇐ had to ⇒ repeatedly ⇐ request a second time from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;<u>;</u></p>	<p>(e) the number of fingerprint data which the Central Unit ⇒ System ⇐ had to ⇒ repeatedly ⇐ request a second time from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;<u>;</u></p>	<p>Identical</p>
<p>(f) the number of requests for marking and unmarking</p>	<p>(f) the number of requests for blocking and unblocking</p>	<p>(f) the number of requests for marking and unmarking</p>	<p>To be reconsidered when Art. 18 is agreed</p>

transmitted in accordance with Article 18(1) and (2).	transmitted in accordance with Article 18(1) and (2).	transmitted in accordance with Article 18(1) and (2).	
(g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under points (b) and (d) of this Article.	(g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under points (b) and (d) of this Article.	(g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under points (b) and (d) of this Article.	Identical
		➤ <u>(h) the number of requests referred to in Article 20 (1)</u> ☛	EP agrees with the Council text
		➤ <u>(i) the number of hits referred to in Article 20 (1)</u> ☛	EP agrees with the Council text
		➤ <u>(j) the number of requests referred to in Article 21 (1)</u> ☛	EP agrees with the Council text
		➤ <u>(k) the number of hits referred to in Article 21 (1)</u> ☛	EP agrees with the Council text
<u>2.</u> At the end of each year, statistical data shall be established in the form of a compilation of the	2. At the end of each year, statistical data shall be established in the form of a compilation of the	<u>2.</u> At the end of each year, statistical data shall be established in the form of a compilation of the	

<p>⇒ monthly ⇐ quarterly statistics drawn up since the beginning of Eurodac's activities ⇒ for that year ⇐, including an indication of the number of persons for whom hits have been recorded under ⇒ points ⇐ (b), (c), and (d). ⇒ The statistics shall contain a breakdown of data for each Member State. ⇐</p>	<p><i>quarterly</i> statistics for that year, including an indication of the number of persons for whom hits have been recorded under points (b), (c), and (d). The statistics shall contain a breakdown of data for each Member State. <i>The result shall be made public.</i></p>	<p>⇒ monthly ⇐ quarterly statistics drawn up since the beginning of Eurodac's activities ⇒ for that year ⇐, including an indication of the number of persons for whom hits have been recorded under ⇒ points ⇐ (b), (c), and (d). ⇒ The statistics shall contain a breakdown of data for each Member State. ⇐</p>	<p>EP amendment is agreed</p> <p>EP amendment is agreed</p>
<p>4. Pursuant to the procedure laid down in Article 23(2), the Central Unit may be charged with carrying out certain other statistical tasks on the basis of the data processed at the Central Unit.</p>	<p>4. Pursuant to the procedure laid down in Article 23(2), the Central Unit may be charged with carrying out certain other statistical tasks on the basis of the data processed at the Central Unit.</p>	<p>4. Pursuant to the procedure laid down in Article 23(2), the Central Unit may be charged with carrying out certain other statistical tasks on the basis of the data processed at the Central Unit.</p>	

<p style="text-align: center;">CHAPTER II</p>	<p style="text-align: center;">CHAPTER II</p>	<p style="text-align: center;">CHAPTER II</p>	
<p style="text-align: center;">APPLICANTS FOR ASYLUM ⊗ INTERNATIONAL PROTECTION ⊗</p>	<p style="text-align: center;">APPLICANTS FOR ASYLUM ⊗ INTERNATIONAL PROTECTION ⊗</p>	<p style="text-align: center;">APPLICANTS FOR ASYLUM ⊗ INTERNATIONAL PROTECTION ⊗</p>	
<p style="text-align: center;"><i>Article 9.4</i> Collection, transmission and comparison of fingerprints</p>	<p style="text-align: center;"><i>Article 9</i> <i>Collection, transmission and comparison of fingerprint data</i></p>	<p style="text-align: center;"><i>Article 9.4</i> Collection, transmission and comparison of fingerprints</p>	<p>It is agreed to maintain the Cion original proposal title.</p>
<p>1. Each Member State shall promptly take the fingerprints of all fingers of every applicant for asylum ⇒ international protection ⇐ of at least 14 years of age and shall promptly ⇒ as soon as possible and no later than 72 hours after the lodging of that application for international protection as defined by Article 20(2) of the Dublin Regulation ⇐ transmit ⊗ them together with ⊗ the data referred to in points (a) (b) to (f)</p>	<p>1. Each Member State shall promptly take the fingerprints of all fingers of every applicant for asylum ⇒ international protection ⇐ of at least 14 years of age and shall promptly ⇒ as soon as possible and no later than 72 hours after the lodging of that application for international protection as defined by Article 20(2) of the Dublin Regulation ⇐ transmit ⊗ them together with ⊗ the data referred to in points (a) (b) to (f)</p>	<p>1. Each Member State shall promptly take the fingerprints of all fingers of every applicant for asylum ⇒ international protection ⇐ of at least 14 years of age and shall promptly ⇒ as soon as possible and no later than 72 hours after the lodging of that application for international protection as defined by Article 20(2) of the Dublin Regulation ⇐ transmit ⊗ them together with ⊗ the data referred to in points (a) (b) to (f)</p>	<p>Identical</p>

<p>(g) of Article 5(1) 11 to the Central Unit ⇒ System ⇐.</p>	<p>(g) of Article 5(1) 11 to the Central Unit ⇒ System ⇐.</p>	<p>(g) of Article 5(1) 11 to the Central Unit ⇒ System ⇐.</p>	
<p>⇒ Non compliance with the 72 hours time limit does 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 to take the fingerprints in a quality ensuring appropriate comparison under Article 25 of this Regulation, 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 taken. ⇐</p>	<p>⇒ Non compliance with the 72 hours time limit does 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 to take the fingerprints in a quality ensuring appropriate comparison under Article 25 of this Regulation, 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 taken. ⇐</p>	<p>⇒ Non compliance with the 72 hours time limit does 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 to take the fingerprints in a quality ensuring appropriate comparison under Article 25 of this Regulation, 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 taken. ⇐</p>	
<p>(2)The data referred to in Article 5(1) shall be immediately recorded in the central database by the Central Unit, or, provided that the technical conditions for</p>	<p>(2)The data referred to in Article 5(1) shall be immediately recorded in the central database by the Central Unit, or, provided that the technical conditions for</p>	<p>(2)The data referred to in Article 5(1) shall be immediately recorded in the central database by the Central Unit, or, provided that the technical conditions for</p>	

<p>such purposes are met, directly by the Member State of origin.</p>	<p>such purposes are met, directly by the Member State of origin.</p>	<p>such purposes are met, directly by the Member State of origin.</p>	
<p>2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.</p>	<p>2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant, <i>for</i> the protection of public health <i>or for technical reasons</i>, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.</p>	<p>2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.</p>	<p>As a result of the third informal trilogue, the EP provisionally accepted the Pres compromise on the provision, which reads as follows.</p> <p>By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these health grounds no longer prevail. In the event of serious technical problems, Member States may extend the original 72-hour deadline in paragraph 1 by a maximum of a further 48 hours in order to execute national continuity plans.</p>
	<p>2a. <i>Temporary or permanent impossibility to provide</i></p>		<p>EP suggestion for a new Recital replacing the amendment to Art. 9</p>

	<p><i>usable fingerprints shall not adversely affect the legal situation of the individual. In any event, such impossibility shall not constitute sufficient grounds to refuse to examine or to reject an application for international protection.</i></p>		<p>and 14:</p> <p><i>"Any temporary or permanent impossibility to take and/or to transmit fingerprint data, due to reasons such as insufficient quality of the data for appropriate comparison, technical problems, reasons linked to protection of health or due to the fact that the data subject is unfit or unable to have his/her fingerprints taken owing to circumstances beyond his/her control, should not adversely affect the examination and the decision on the application for international protection lodged by this person."</i></p> <p>EP amendment accepted by Council</p>
<p>3. Fingerprint data within the meaning of point (b) <u>(a)</u> of Article 5(1) <u>11</u>, transmitted by any Member State, <input checked="" type="checkbox"/> with exception to those transmitted in accordance with Article 10 point (b) <input checked="" type="checkbox"/> shall be compared <input type="checkbox"/> automatically <input type="checkbox"/> with</p>	<p>3. Fingerprint data within the meaning of point (b) <u>(a)</u> of Article 5(1) <u>11</u>, transmitted by any Member State, <input checked="" type="checkbox"/> with exception to those transmitted in accordance with Article 10 point (b) <input checked="" type="checkbox"/> shall be compared <input type="checkbox"/> automatically <input type="checkbox"/> with</p>	<p>3. Fingerprint data within the meaning of point (b) <u>(a)</u> of Article 5(1) <u>11</u>, transmitted by any Member State, <input checked="" type="checkbox"/> with exception to those transmitted in accordance with Article 10 point (b) <input checked="" type="checkbox"/> shall be compared by the Central Unit</p>	<p>Identical</p>

<p>the fingerprint data transmitted by other Member States and already stored in the <u>Central database</u> ⇒ System ⇐.</p>	<p>the fingerprint data transmitted by other Member States and already stored in the <u>Central database</u> ⇒ System ⇐.</p>	<p>⇒ automatically ⇐ with the fingerprint data transmitted by other Member States and already stored in the <u>Central database</u> ⇒ System ⇐.</p>	
<p>4. The Central <u>Unit</u> ⇒ System ⇐ shall ensure, on 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.</p>	<p>4. The Central <u>Unit</u> ⇒ System ⇐ shall ensure, on 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.</p>	<p>4. The Central <u>Unit</u> ⇒ System ⇐ shall ensure, on 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.</p>	<p>Identical</p>
<p>5. The Central <u>Unit</u> ⇒ System ⇐ shall forthwith ⇒ 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 5(1) 8(a) to</p>	<p>5. The Central <u>Unit</u> ⇒ System ⇐ shall forthwith ⇒ 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 5(1) 8(a) to</p>	<p>5. The Central <u>Unit</u> ⇒ System ⇐ shall forthwith ⇒ 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 ... <u>Articles</u></p>	

<p>(⇒ g ⇐) although in the case of the data referred to in Article 5(1)(b), only insofar as they were the basis for the hit ⇐ along with, where appropriate, the mark referred to in Article 18(1) ⇐.</p>	<p>(⇒ g ⇐) although in the case of the data referred to in Article 5(1)(b), only insofar as they were the basis for the hit ⇐ along with, where appropriate, the mark referred to in Article 18(1) ⇐.</p>	<p>5(1) ⇐ [...] ⇐ 11 ⇐ (a) to (⇒ ⇐ [...] ⇐ k ⇐ ⇐) although in the case of the data referred to in Article 5(1)(b), only insofar as they were the basis for the hit ⇐ along with, where appropriate, the mark referred to in Article 18(1) ⇐.</p>	<p>Technical - agreed</p>
<p>Direct transmission to the Member State of origin of the result of the comparison shall be permissible where the technical conditions for such purpose are met.</p>	<p>Direct transmission to the Member State of origin of the result of the comparison shall be permissible where the technical conditions for such purpose are met.</p>	<p>Direct transmission to the Member State of origin of the result of the comparison shall be permissible where the technical conditions for such purpose are met.</p>	
<p>7. The implementing rules setting out the procedures necessary for the application of paragraphs 1 to 6 shall be adopted in accordance with the procedure laid down in Article 22(1).</p>	<p>7. The implementing rules setting out the procedures necessary for the application of paragraphs 1 to 6 shall be adopted in accordance with the procedure laid down in Article 22(1).</p>	<p>7. The implementing rules setting out the procedures necessary for the application of paragraphs 1 to 6 shall be adopted in accordance with the procedure laid down in Article 22(1).</p>	
<p><i>Article 10</i> Information on the status of the data subject</p>	<p><i>Article 10</i> Information on the status of the data subject</p>	<p><i>Article 10</i> Information on the status of the data subject</p>	
<p>The following</p>	<p>The following</p>	<p>The following</p>	

<p>information shall be sent to the Central System in order to be stored in accordance with Article 9 for the purpose of transmission under Article 9(5):</p>	<p>information shall be sent to the Central System in order to be stored in accordance with Article 9 for the purpose of transmission under Article 9(5):</p>	<p>information shall be sent to the Central System in order to be stored in accordance with Article 12 [...] for the purpose of transmission under Article 9(5):</p>	<p>Technical - agreed</p>
<p>(a) When an applicant for international protection or another person as referred to in point (d) of Article 18(1) of the Dublin Regulation arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take him/her back as referred to in Article 24 of the Dublin Regulation, the responsible Member State shall update its dataset recorded in conformity with Article 8 of this Regulation relating to the person concerned by adding their date of arrival .</p>	<p>(a) When an applicant for international protection or another person as referred to in point (d) of Article 18(1) of the Dublin Regulation arrives in the responsible Member State following a transfer pursuant to a request to take him/her back as referred to in Article 24 of the Dublin Regulation, the responsible Member State shall update its dataset recorded in conformity with Article 8 of this Regulation relating to the person concerned by adding their date of arrival .</p>	<p>(a) When an applicant for international protection or another person as referred to in point (d) of Article 18(1) of the Dublin Regulation arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take him/her back as referred to in Article 24 of the Dublin Regulation, the responsible Member State shall update its dataset recorded in conformity with Article [...] of this Regulation relating to the person concerned by adding their date of arrival .</p>	<p>Technical - reference should be made to Art. 25 of the Dublin Regulation</p> <p>Technical - agreed</p>

<p>(b) When an applicant for international protection arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take charge of them as referred to in Article 22 of the Dublin Regulation, the responsible Member State shall send a dataset in conformity with Article 11 of this Regulation relating to the person concerned and include their date of arrival.</p>	<p>(b) When an applicant for international protection arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take charge of them as referred to in Article 22 of the Dublin Regulation, the responsible Member State shall send a dataset in conformity with Article 11 of this Regulation relating to the person concerned and include their date of arrival.</p>	<p>(b) When an applicant for international protection arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take charge of [...] him/her as referred to in Article 22 of the Dublin Regulation, the responsible Member State shall send a dataset in conformity with Article 11 of this Regulation relating to the person concerned and include their date of arrival.</p>	<p>Technical - agreed</p>
<p>(c) As soon as the Member State of origin can establish 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 dataset recorded in conformity with Article 11 of this</p>	<p>(c) As soon as the Member State of origin can establish 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 dataset recorded in conformity with Article 11 of this</p>	<p>(c) As soon as the Member State of origin can establish 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 dataset recorded in conformity with Article 11 of this</p>	<p>Identical</p>

<p>Regulation relating to the person concerned by adding the date when the person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of the Dublin Regulation.</p>	<p>Regulation relating to the person concerned by adding the date when the person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of the Dublin Regulation.</p>	<p>Regulation relating to the person concerned by adding the date when the person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of the Dublin Regulation.</p>	
<p>(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 has left the territory of the Member States in compliance with a return decision or removal order it issued following the withdrawal or rejection of the application as provided for in Article 19(3) of the Dublin Regulation, it shall update its dataset recorded in conformity with Article 11 relating to the person concerned by adding the date of his/her removal or when the person left the territory.</p>	<p>(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 has left the territory of the Member States in compliance with a return decision or removal order it issued following the withdrawal or rejection of the application as provided for in Article 19(3) of the Dublin Regulation, it shall update its dataset recorded in conformity with Article 11 relating to the person concerned by adding the date of his/her removal or when the person left the territory.</p>	<p>(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 has left the territory of the Member States in compliance with a return decision or removal order it issued following the withdrawal or rejection of the application as provided for in Article 19(3) of the Dublin Regulation, it shall update its dataset recorded in conformity with Article 11 relating to the person concerned by adding the date of his/her removal or when the person left the territory.</p>	<p>Identical</p>

<p>(e) The Member State which assumes responsibility in accordance with Article 17(1) of the Dublin Regulation shall update its dataset recorded in conformity with Article 11 of this Regulation relating to that applicant by adding the date when the decision to examine the application was taken.</p>	<p>(e) The Member State which assumes responsibility in accordance with Article 17(1) of the Dublin Regulation shall update its dataset recorded in conformity with Article 11 of this Regulation relating to that applicant by adding the date when the decision to examine the application was taken.</p>	<p>(e) The Member State which assumes responsibility in accordance with Article 17(1) of the Dublin Regulation shall update its dataset recorded in conformity with Article 11 of this Regulation relating to that applicant by adding the date when the decision to examine the application was taken.</p>	<p>Identical</p>
<p><i>Article 11 §</i> Recording of data</p>	<p><i>Article 11 §</i> Recording of data</p>	<p><i>Article 11 §</i> Recording of data</p>	
<p>1 Only the following data shall be recorded in the <u>eCentral</u> database ⇒ System ⇐ :</p>	<p>1 Only the following data shall be recorded in the <u>eCentral</u> database ⇒ System ⇐ :</p>	<p>1 Only the following data shall be recorded in the <u>eCentral</u> database ⇒ System ⇐ :</p>	<p>Identical</p>
<p>(ab) fingerprint data;</p>	<p>(ab) fingerprint data;</p>	<p>(ab) fingerprint data;</p>	
<p>(ba) Member State of origin, place and date of the application for asylum ⇒ international protection; in the cases referred to in point (b) of Article</p>	<p>(ba) Member State of origin, place and date of the application for asylum ⇒ international protection; in the cases referred to in point (b) of Article</p>	<p>(ba) Member State of origin, place and date of the application for asylum ⇒ international protection; in the cases referred to in point (b) of Article</p>	

10, the date of application shall be the one entered by the Member State who transferred the applicant ⇄;	10, the date of application shall be the one entered by the Member State who transferred the applicant ⇄;	10, the date of application shall be the one entered by the Member State who transferred the applicant ⇄;	
(c) sex;	(c) sex;	(c) sex;	
(d) reference number used by the Member State of origin;	(d) reference number used by the Member State of origin;	(d) reference number used by the Member State of origin;	
(e) date on which the fingerprints were taken;	(e) date on which the fingerprints were taken;	(e) date on which the fingerprints were taken;	
(f) date on which the data were transmitted to the Central Unit ⇄ System ⇄;	(f) date on which the data were transmitted to the Central Unit ⇄ System ⇄;	(f) date on which the data were transmitted to the Central Unit ⇄ System ⇄;	
(g) date on which the data were entered in the central database;	(g) date on which the data were entered in the central database;	(g) date on which the data were entered in the central database;	
(g) operator user ID.	(g) operator user ID.	(g) operator user ID.	
(h) details in respect of the recipient(s) of the data transmitted and the date(s) of	(h) details in respect of the recipient(s) of the data transmitted and the date(s) of	(h) details in respect of the recipient(s) of the data transmitted and the date(s) of	

transmission(s).	transmission(s).	transmission(s).	
(h) where applicable in accordance with Article 10 point (a) or point (b), the date of the arrival of the person concerned after a successful transfer;	(h) where applicable in accordance with Article 10 point (a) or point (b), the date of the arrival of the person concerned after a successful transfer;	(h) where applicable in accordance with Article 10 point (a) or point (b), the date of the arrival of the person concerned after a successful transfer;	
(i) where applicable in accordance with Article 10 point (c), the date when the person concerned left the territory of the Member States;	(i) where applicable in accordance with Article 10 point (c), the date when the person concerned left the territory of the Member States;	(i) where applicable in accordance with Article 10 point (c), the date when the person concerned left the territory of the Member States;	
(j) where applicable in accordance with Article 10 point (d), the date when the person concerned left or was removed from the territory of the Member States;	(j) where applicable in accordance with Article 10 point (d), the date when the person concerned left or was removed from the territory of the Member States;	(j) where applicable in accordance with Article 10 point (d), the date when the person concerned left or was removed from the territory of the Member States;	
(k) where applicable in accordance with Article 10 point (e), the date when the decision to examine	(k) where applicable in accordance with Article 10 point (e), the date when the decision to examine	(k) where applicable in accordance with Article 10 point (e), the date when the decision to examine	

the application was taken.	the application was taken.	the application was taken.	
2. After recording the data in the central database, the Central Unit shall destroy the media used for transmitting the data, unless the Member State of origin has requested their return.	2. After recording the data in the central database, the Central Unit shall destroy the media used for transmitting the data, unless the Member State of origin has requested their return.	2. After recording the data in the central database, the Central Unit shall destroy the media used for transmitting the data, unless the Member State of origin has requested their return.	
<i>Article 12</i> 6 Data storage	<i>Article 12</i> 6 Data storage	<i>Article 12</i> 6 Data storage	
Each set of data, as referred to in Article 5(1) 11, shall be stored in the Central ⇒ System ⇐ database for ten years from the date on which the fingerprints were taken.	Each set of data, as referred to in Article 5(1) 11, shall be stored in the Central ⇒ System ⇐ database for ten years from the date on which the fingerprints were taken.	Each set of data, as referred to in Article 5(1) 11, shall be stored in the Central ⇒ System ⇐ database for ten years from the date on which the fingerprints were taken.	Identical
Upon expiry of this period, the Central Unit ⇒ System ⇐ shall automatically erase the data from the Central	Upon expiry of this period, the Central Unit ⇒ System ⇐ shall automatically erase the data from the Central	Upon expiry of this period, the Central Unit ⇒ System ⇐ shall automatically erase the data from the Central	

database ⇒ System ⇐.	database ⇒ System ⇐.	database ⇒ System ⇐.	
<i>Article 13</i> 7 Advance data erasure	<i>Article 13</i> 7 Advance data erasure	<i>Article 13</i> 7 Advance data erasure	
1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article 6 <u>12</u> shall be erased from the Central Unit ⇒ System ⇐, in accordance with Article 15(3) <u>27(4)</u> as soon as the Member State of origin becomes aware that the person has acquired such citizenship.	1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article 6 <u>12</u> shall be erased from the Central Unit ⇒ System ⇐, in accordance with Article 15(3) <u>27(4)</u> as soon as the Member State of origin becomes aware that the person has acquired such citizenship.	1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article 6 <u>12</u> shall be erased from the Central Unit ⇒ System ⇐, in accordance with Article 15(3) <u>27(4)</u> as soon as the Member State of origin becomes aware that the person has acquired such citizenship.	Identical
2. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in	2. The Central System shall inform <i>as soon as possible and not later than after 72 hours</i> , all Member States of origin about the erasure of data for the reason specified in paragraph 1 by another Member State of origin having produced a hit with data which they	2. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in paragraph 1 by another Member State of origin having produced a hit with data which they	EP amendment accepted by Council

Article 9(1) or Article 14(1).	transmitted relating to persons referred to in Article 9(1) or Article 14(1).	Article 9(1) or Article 14(1).	
CHAPTER III	CHAPTER III	CHAPTER III	
ALIENS ☒ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ☒ APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER	ALIENS ☒ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ☒ APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER	ALIENS ☒ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ☒ APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER	
<i>Article 14</i> § Collection and transmission of fingerprint data	<i>Article 14</i> § Collection and transmission of fingerprint data	<i>Article 14</i> § Collection and transmission of fingerprint data	
1. Each Member State shall, in accordance with the safeguards laid down in the European Convention on Human Rights and in	1. Each Member State shall, <i>whilst fully respecting the safeguards laid down in the Charter of Fundamental Rights of</i>	1. Each Member State shall, in accordance with the safeguards laid down in the European Convention on Human Rights and in	EP accepts the Council text

<p>the United Nations Convention on the Rights of the Child promptly take the fingerprints of all fingers of every alien ☒ third country national or stateless person ☒ of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back ⇒ or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn them back ⇐ .</p>	<p><i>the European Union, the European Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations Convention on the Rights of the Child,</i> promptly take the fingerprints of all fingers of every third country national or stateless person of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of</p>	<p>the United Nations Convention on the Rights of the Child promptly take the fingerprints of all fingers of every alien ☒ third country national or stateless person ☒ of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back ⇒ or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn them back ⇐ .</p>	
---	--	---	--

	the decision to turn <i>him or her</i> back.		
2. The Member State concerned shall promptly ⇒ as soon as possible and no later than 72 hours from the date of apprehension ⇐ transmit to the Central Unit ⇒ System ⇐ the following data in relation to any alien ⊗ third country national or stateless person ⊗, as referred to in paragraph 1, who is not turned back:	2. The Member State concerned shall promptly ⇒ as soon as possible and no later than 72 hours from the date of apprehension ⇐ transmit to the Central Unit ⇒ System ⇐ the following data in relation to any alien ⊗ third country national or stateless person ⊗, as referred to in paragraph 1, who is not turned back:	2. The Member State concerned shall promptly ⇒ as soon as possible and no later than 72 hours from the date of apprehension ⇐ transmit to the Central Unit ⇒ System ⇐ the following data in relation to any alien ⊗ third country national or stateless person ⊗, as referred to in paragraph 1, who is not turned back:	Identical
(ab) fingerprint data;	(ab) fingerprint data;	(ab) fingerprint data;	
(ba) Member State of origin, place and date of the apprehension;	(ba) Member State of origin, place and date of the apprehension;	(ba) Member State of origin, place and date of the apprehension;	
(c) sex;	(c) sex;	(c) sex;	
(d) reference number used by the Member State of origin;	(d) reference number used by the Member State of origin;	(d) reference number used by the Member State of origin;	

(e) date on which the fingerprints were taken;	(e) date on which the fingerprints were taken;	(e) date on which the fingerprints were taken;	
(f) date on which the data were transmitted to the Central Unit ⇒ System ⇐;	(f) date on which the data were transmitted to the Central Unit ⇒ System ⇐;	(f) date on which the data were transmitted to the Central Unit ⇒ System ⇐;	
(g) operator user ID.	(g) operator user ID.	(g) operator user ID.	
3. By way of derogation from paragraph 2, as regards persons apprehended in the manner 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, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their release from custody, confinement or detention.	3. By way of derogation from paragraph 2, as regards persons apprehended in the manner 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, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their release from custody, confinement or detention.	3. By way of derogation from paragraph 2, as regards persons apprehended in the manner 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, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their release from custody, confinement or detention.	Identical

<p>4. Non compliance with the 72 hours time limit referred to in paragraph 2 does 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 to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.</p>	<p>4. [...] Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.</p>	<p>4. Non compliance with the 72 hours time limit referred to in paragraph 2 does 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 to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.</p>	<p>EP accepts the Council text</p>
<p>5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person or the protection of public health, the Member State concerned shall take and send the</p>	<p>5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person, <i>for</i> the protection of public health <i>or for technical reasons</i>, the Member State concerned</p>	<p>5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person or the protection of public health, the Member State concerned shall take and send the</p>	<p>As a result of the third informal trilogue, the EP provisionally accepted the Pres compromise on the provision, which reads as follows:</p> <p>By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the</p>

<p>fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.</p>	<p>shall take and send the fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.</p>	<p>fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.</p>	<p>health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these health grounds no longer prevail. In the event of serious technical problems, Member States may extend the original 72-hour deadline in paragraph 1 by a maximum of a further 48 hours in order to execute national continuity plans.</p>
	<p><i>5a. Temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any event, such impossibility shall not constitute sufficient grounds to refuse to examine or to reject an application for international protection.</i></p>		<p>(See comments on Art. 9(2a) EP amendment to be deleted</p>
<p><i>Article 15</i> 9 Recording of data</p>	<p><i>Article 15</i> 9 Recording of data</p>	<p><i>Article 15</i> 9 Recording of data</p>	
<p>1. The data referred to in</p>	<p>1. The data referred to in</p>	<p>1. The data referred to in</p>	<p>Identical</p>

<p>Article 5(1)(g) and in Article 8(2) <u>14(2)</u> shall be recorded in the central database ⇒ Central System ⇐.</p>	<p>Article 5(1)(g) and in Article 8(2) <u>14(2)</u> shall be recorded in the central database ⇒ Central System ⇐.</p>	<p>Article 5(1)(g) and in Article 8(2) <u>14(2)</u> shall be recorded in the central database ⇒ Central System ⇐.</p>	
<p>Without prejudice to Article 3(3)<u>8</u>, data transmitted to the Central Unit ⇒ System ⇐ pursuant to Article 8(2) <u>14(2)</u> shall be recorded for the sole purpose of comparison with data on applicants for asylum ⇒ international protection ⇐ transmitted subsequently to the Central Unit ⇒ System ⇐.</p>	<p>Without prejudice to Article 3(3)<u>8</u>, data transmitted to the Central Unit ⇒ System ⇐ pursuant to Article 8(2) <u>14(2)</u> shall be recorded for the sole purpose of comparison with data on applicants for asylum ⇒ international protection ⇐ transmitted subsequently to the Central Unit ⇒ System ⇐.</p>	<p>Without prejudice to Article 3(3)<u>8</u>, data transmitted to the Central Unit ⇒ System ⇐ pursuant to Article 8(2) <u>14(2)</u> shall be recorded for the sole purpose of comparison with data on applicants for asylum ⇒ international protection ⇐ transmitted subsequently to the Central Unit ⇒ System ⇐ and for the purposes as laid down in Article 1(2) ⊖ .</p>	<p>As a result of the third informal trilogue, EP and Council provisionally agreed, for clarification purposes to amend the wording of the provision as follows:</p> <p>"... shall be recorded solely for the purposes of comparison with data on applicants for asylum ⇒ international protection ⇐ and the purposes laid down in Art. 1(2) transmitted subsequently to the Central Unit ⇒ System ⇐ ⊕</p>
<p>The Central Unit ⇒ System ⇐ shall not compare data transmitted to it pursuant to Article 8(2) <u>14(2)</u> with any data previously recorded in the central database ⇒ Central System ⇐, nor with data subsequently transmitted to the Central</p>	<p>The Central Unit ⇒ System ⇐ shall not compare data transmitted to it pursuant to Article 8(2) <u>14(2)</u> with any data previously recorded in the central database ⇒ Central System ⇐, nor with data subsequently transmitted to the Central</p>	<p>The Central Unit ⇒ System ⇐ shall not compare data transmitted to it pursuant to Article 8(2) <u>14(2)</u> with any data previously recorded in the central database ⇒ Central System ⇐, nor with data subsequently transmitted to the Central</p>	

<p>Unit ⇨ System ⇨ pursuant to Article 8(2) 14(2).</p>	<p>Unit ⇨ System ⇨ pursuant to Article 8(2) 14(2).</p>	<p>Unit ⇨ System ⇨ pursuant to Article 8(2) 14(2).</p>	
<p>2. The procedures provided for in Article 4(1), second sentence, Article 4(2) and Article 5(2) as well as the provisions laid down pursuant to Article 4(7) shall apply. As regards the comparison of data on applicants for asylum ⇨ international protection ⇨ subsequently transmitted to the Central Unit ⇨ System ⇨ with the data referred to in paragraph 1, the procedures provided for in Article 4(3), (5) and (6) 9(3) and (5) and in <u>Article 25(4)</u> shall apply.</p>	<p>2. The procedures provided for in Article 4(1), second sentence, Article 4(2) and Article 5(2) as well as the provisions laid down pursuant to Article 4(7) shall apply. As regards the comparison of data on applicants for asylum ⇨ international protection ⇨ subsequently transmitted to the Central Unit ⇨ System ⇨ with the data referred to in paragraph 1, the procedures provided for in Article 4(3), (5) and (6) 9(3) and (5) and in <u>Article 25(4)</u> shall apply.</p>	<p>2. The procedures provided for in Article 4(1), second sentence, Article 4(2) and Article 5(2) as well as the provisions laid down pursuant to Article 4(7) shall apply. As regards the comparison of data on applicants for asylum ⇨ international protection ⇨ subsequently transmitted to the Central Unit ⇨ System ⇨ with the data referred to in paragraph 1, the procedures provided for in Article 4(3), (5) and (6) 9(3) and (5) and in <u>Article 25(4)</u> shall apply.</p>	<p>Identical</p>
<p><i>Article 16 10</i> Storage of data</p>	<p><i>Article 16 10</i> Storage of data</p>	<p><i>Article 16 10</i> Storage of data</p>	
<p>1. Each set of data relating to an alien ☒ third country national or stateless person ☒ as</p>	<p>1. Each set of data relating to an alien ☒ third country national or stateless person ☒ as</p>	<p>1. Each set of data relating to an alien ☒ third country national or stateless person ☒ as</p>	

<p>referred to in Article 8(1) <u>14(1)</u> shall be stored in the central database ⇒ Central System ⇐ for ⇒ one year ⇐ two years from the date on which the fingerprints of the alien ⊗ third country national or stateless person ⊗ were taken. Upon expiry of this period, the Central Unit ⇒ System ⇐ shall automatically erase the data from the central database ⇒ Central System ⇐.</p>	<p>referred to in Article 8(1) <u>14(1)</u> shall be stored in the central database ⇒ Central System ⇐ for ⇒ one year ⇐ two years from the date on which the fingerprints of the alien ⊗ third country national or stateless person ⊗ were taken. Upon expiry of this period, the Central Unit ⇒ System ⇐ shall automatically erase the data from the central database ⇒ Central System ⇐.</p>	<p>referred to in Article 8(1) <u>14(1)</u> shall be stored in the central database ⇒ Central System ⇐ for ⇒ two <u>[...]</u> two years ⇐ ⇐ two years from the date on which the fingerprints of the alien ⊗ third country national or stateless person ⊗ were taken. Upon expiry of this period, the Central Unit ⇒ System ⇐ shall automatically erase the data from the central database ⇒ Central System ⇐.</p>	<p>Council maintains its preference for a two-year storage. EP insists on a storage period of one year.</p> <p>The Pres recommends a storage period of 18 months as a compromise, with regard to working out an overall compromise.</p>
<p>2. The data relating to an an alien ⊗ third country national or stateless person ⊗ as referred to in Article 8(1) <u>14(1)</u> shall be erased from the central database ⇒ Central System ⇐ in accordance with Article 15(3) <u>28(3)</u> ⊗ as soon as ⊗ the Member State of origin becomes aware of one of the following circumstances before the</p>	<p>2. The data relating to an an alien ⊗ third country national or stateless person ⊗ as referred to in Article 8(1) <u>14(1)</u> shall be erased from the central database ⇒ Central System ⇐ in accordance with Article 15(3) <u>28(3)</u> ⊗ as soon as ⊗ the Member State of origin becomes aware of one of the following circumstances before the</p>	<p>2. The data relating to an an alien ⊗ third country national or stateless person ⊗ as referred to in Article 8(1) <u>14(1)</u> shall be erased from the central database ⇒ Central System ⇐ in accordance with Article 15(3) <u>27</u> (3) ⊗ as soon as ⊗ the Member State of origin becomes aware of one of the following</p>	

<p>two ⇒ one ←-year period mentioned in paragraph 1 has expired:</p>	<p>two ⇒ one ←-year period mentioned in paragraph 1 has expired:</p>	<p>circumstances before the two ⇒ two [...] ←-year period mentioned in paragraph 1 has expired:</p>	<p>see above - para. 1</p>
<p>(a) the alien ☒ third country national or stateless person ☒ has been issued with a residence permit ☒ document ☒ ;</p>	<p>(a) the alien ☒ third country national or stateless person ☒ has been issued with a residence permit ☒ document ☒ ;</p>	<p>(a) the alien ☒ third country national or stateless person ☒ has been issued with a residence permit ☒ document ☒ ;</p>	
<p>(b) the alien ☒ third country national or stateless person ☒ has left the territory of the Member States;</p>	<p>(b) the alien ☒ third country national or stateless person ☒ has left the territory of the Member States;</p>	<p>(b) the alien ☒ third country national or stateless person ☒ has left the territory of the Member States;</p>	
<p>(c) the alien ☒ third country national or stateless person ☒ has acquired the citizenship of any Member State.</p>	<p>(c) the alien ☒ third country national or stateless person ☒ has acquired the citizenship of any Member State.</p>	<p>(c) the alien ☒ third country national or stateless person ☒ has acquired the citizenship of any Member State.</p>	
<p>3. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point</p>	<p>3. The Central System shall inform all Member States of origin <i>as soon as possible and no later than after 72 hours</i></p>	<p>3. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point</p>	<p>EP text is accepted</p>

<p>(a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).</p>	<p>about the erasure of data for the reason specified in point (a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).</p>	<p>(a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).</p>	
<p>4. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (c) of paragraph 2 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 Article 14(1).</p>	<p>4. The Central System shall inform all Member States of origin <i>as soon as possible and no later than after 72 hours</i> about the erasure of data for the reason specified in point (c) of paragraph 2 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 Article 14(1).</p>	<p>4. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (c) of paragraph 2 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 Article 14(1).</p>	<p>EP text is accepted</p>

CHAPTER IV	CHAPTER IV	CHAPTER IV	
<p>ALIENS ☒ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ☒ FOUND ILLEGALLY PRESENT ☒ STAYING ☒ IN A MEMBER STATE</p>	<p>ALIENS ☒ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ☒ FOUND ILLEGALLY PRESENT ☒ STAYING ☒ IN A MEMBER STATE</p>	<p>ALIENS ☒ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ☒ FOUND ILLEGALLY PRESENT ☒ STAYING ☒ IN A MEMBER STATE</p>	
<p><i>Article 17 II</i> Comparison of fingerprint data</p>	<p><i>Article 17 II</i> Comparison of fingerprint data</p>	<p><i>Article 17 II</i> Comparison of fingerprint data</p>	
<p>1. With a view to checking whether an alien ☒ third country national or a stateless person ☒ found illegally present ☒ staying ☒ within its territory has previously lodged an application for asylum ⇒ international protection ⇐ in another Member State, each Member State may</p>	<p>1. With a view to checking whether an alien ☒ third country national or a stateless person ☒ found illegally present ☒ staying ☒ within its territory has previously lodged an application for asylum ⇒ international protection ⇐ in another Member State, each Member State may</p>	<p>1. With a view to checking whether an alien ☒ third country national or a stateless person ☒ found illegally present ☒ staying ☒ within its territory has previously lodged an application for asylum ⇒ international protection ⇐ in another Member State, each Member State may</p>	Identical

<p>transmit to the Central Unit ⇒ System ⇐ any fingerprint data relating to fingerprints which it may have taken of any such alien ⊗ third country national or stateless person ⊗ of at least 14 years of age together with the reference number used by that Member State.</p>	<p>transmit to the Central Unit ⇒ System ⇐ any fingerprint data relating to fingerprints which it may have taken of any such alien ⊗ third country national or stateless person ⊗ of at least 14 years of age together with the reference number used by that Member State.</p>	<p>transmit to the Central Unit ⇒ System ⇐ any fingerprint data relating to fingerprints which it may have taken of any such alien ⊗ third country national or stateless person ⊗ of at least 14 years of age together with the reference number used by that Member State.</p>	
<p>As a general rule there are grounds for checking whether the alien ⊗ third country national or stateless person ⊗ has previously lodged an application for asylum ⇒ international protection ⇐ in another Member State where:</p>	<p>As a general rule there are grounds for checking whether the alien ⊗ third country national or stateless person ⊗ has previously lodged an application for asylum ⇒ international protection ⇐ in another Member State where:</p>	<p>As a general rule there are grounds for checking whether the alien ⊗ third country national or stateless person ⊗ has previously lodged an application for asylum ⇒ international protection ⇐ in another Member State where:</p>	
<p>(a) the alien ⊗ third country national or stateless person ⊗ declares that he/she has lodged an application for asylum ⇒ international protection ⇐ but</p>	<p>(a) the alien ⊗ third country national or stateless person ⊗ declares that he/she has lodged an application for asylum ⇒ international protection ⇐ but</p>	<p>(a) the alien ⊗ third country national or stateless person ⊗ declares that he/she has lodged an application for asylum ⇒ international protection ⇐ but</p>	

<p>without indicating the Member State in which he/she made the application;</p>	<p>without indicating the Member State in which he/she made the application;</p>	<p>without indicating the Member State in which he/she made the application;</p>	
<p>(b) the alien ☒ third country national or stateless person ☒ does not request asylum ⇒ international protection ☐ but objects to being returned to his/her country of origin by claiming that he/she would be in danger, or</p>	<p>(b) the alien ☒ third country national or stateless person ☒ does not request asylum ⇒ international protection ☐ but objects to being returned to his/her country of origin by claiming that he/she would be in danger, or</p>	<p>(b) the alien ☒ third country national or stateless person ☒ does not request asylum ⇒ international protection ☐ but objects to being returned to his/her country of origin by claiming that he/she would be in danger, or</p>	
<p>(c) the alien ☒ third country national or stateless person ☒ otherwise seeks to prevent his/her removal by refusing to cooperate in establishing his/her identity, in particular by showing no, or false, identity papers.</p>	<p>(c) the alien ☒ third country national or stateless person ☒ otherwise seeks to prevent his/her removal by refusing to cooperate in establishing his/her identity, in particular by showing no, or false, identity papers.</p>	<p>(c) the alien ☒ third country national or stateless person ☒ otherwise seeks to prevent his/her removal by refusing to cooperate in establishing his/her identity, in particular by showing no, or false, identity papers.</p>	

<p>2. Where Member States take part in the procedure referred to in paragraph 1, they shall transmit to the Central Unit ⇒ System ⇐ the fingerprint data relating to all or at least the index fingers, and, if those are missing, the prints of all other fingers, of aliens ⊗ third country nationals or stateless persons ⊗ referred to in paragraph 1.</p>	<p>2. Where Member States take part in the procedure referred to in paragraph 1, they shall transmit to the Central Unit ⇒ System ⇐ the fingerprint data relating to all or at least the index fingers, and, if those are missing, the prints of all other fingers, of aliens ⊗ third country nationals or stateless persons ⊗ referred to in paragraph 1.</p>	<p>2. Where Member States take part in the procedure referred to in paragraph 1, they shall transmit to the Central Unit ⇒ System ⇐ the fingerprint data relating to all or at least the index fingers, and, if those are missing, the prints of all other fingers, of aliens ⊗ third country nationals or stateless persons ⊗ referred to in paragraph 1.</p>	<p>Identical</p>
<p>3. The fingerprint data of an alien ⊗ third country national or a stateless person ⊗ as referred to in paragraph 1 shall be transmitted to the Central Unit ⇒ System ⇐ solely for the purpose of comparison with the fingerprint data of applicants for asylum ⇒ international protection ⇐ transmitted by other Member States and already recorded in the central database</p>	<p>3. The fingerprint data of an alien ⊗ third country national or a stateless person ⊗ as referred to in paragraph 1 shall be transmitted to the Central Unit ⇒ System ⇐ solely for the purpose of comparison with the fingerprint data of applicants for asylum ⇒ international protection ⇐ transmitted by other Member States and already recorded in the central database</p>	<p>3. The fingerprint data of an alien ⊗ third country national or a stateless person ⊗ as referred to in paragraph 1 shall be transmitted to the Central Unit ⇒ System ⇐ solely for the purpose of comparison with the fingerprint data of applicants for asylum ⇒ international protection ⇐ transmitted by other Member States and already recorded in the central database</p>	<p>Identical</p>

⇒ Central System ⇐.	⇒ Central System ⇐.	⇒ Central System ⇐.	
<p>The fingerprint data of such an alien ☒ third country national or a stateless person ☒ shall not be recorded in the central database ⇒ Central System ⇐, nor shall they be compared with the data transmitted to the Central Unit ⇒ System ⇐ pursuant to Article 8(2) 14(2).</p>	<p>The fingerprint data of such an alien ☒ third country national or a stateless person ☒ shall not be recorded in the central database ⇒ Central System ⇐, nor shall they be compared with the data transmitted to the Central Unit ⇒ System ⇐ pursuant to Article 8(2) 14(2).</p>	<p>The fingerprint data of such an alien ☒ third country national or a stateless person ☒ shall not be recorded in the central database ⇒ Central System ⇐, nor shall they be compared with the data transmitted to the Central Unit ⇒ System ⇐ pursuant to Article 8(2) 14(2).</p>	
<p>4. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for asylum ⇒ international protection ⇐ transmitted by other Member States which have already been stored in the Central Unit ⇒ System ⇐, the procedures provided for in Article 4(3) (5) and (6) 9(3) and (5) as well as the provisions laid down pursuant to Article 4(7) shall apply.</p>	<p>4. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for asylum ⇒ international protection ⇐ transmitted by other Member States which have already been stored in the Central Unit ⇒ System ⇐, the procedures provided for in Article 4(3) (5) and (6) 9(3) and (5) as well as the provisions laid down pursuant to Article 4(7) shall apply.</p>	<p>4. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for asylum ⇒ international protection ⇐ transmitted by other Member States which have already been stored in the Central Unit ⇒ System ⇐, the procedures provided for in Article 4(3) (5) and (6) 9(3) and (5) as well as the provisions pursuant to Article 25 (4) C as well as the provisions laid</p>	<p>Technical - Council text agreed</p>

		<p>down pursuant to Article 4(7) shall apply.</p>	
	<p><i>4a. Once the results of the comparison have been transmitted to the Member State of origin, the Central System shall immediately erase the fingerprint data and other data transmitted to it pursuant to paragraph 1.</i></p>		<p>By way of compromise, the Cion suggests the following compromise (which [should be moved up to become Article 17 (3a)] (in bold, underline):</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 with the fingerprint data of applicants for international protection transmitted by other Member States and already recorded in the Central System.</p> <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> <p><i>Once the results of the comparison have been transmitted to the</i></p>

			<p><i>Member State of origin, the record of the search shall be kept by the EURODAC Central System and the national competent authorities only for the purposes pursuant to Article 28 of permitting the national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union and national data protection rules, including for the purpose of maintaining records in order to draft the reports specified in Article 40(1). Other than for the above-mentioned purposes, no other record of the search may be stored either by Member States or by the Central System.</i></p> <p>The Cion compromise is provisionally acceptable</p>
<p>5. Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:</p>	<p>5. Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:</p>	<p>5. Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:</p>	
<p>(a) erase the fingerprint data and other data transmitted to it</p>	<p>(a) erase the fingerprint data and other data transmitted to it</p>	<p>(a) erase the fingerprint data and other data transmitted to it</p>	

under paragraph 1; and	under paragraph 1; and	under paragraph 1; and	
(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.	(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.	(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.	
CHAPTER V	CHAPTER V	CHAPTER V	
RECOGNISED REFUGEES <input checked="" type="checkbox"/> PERSONS GRANTED INTERNATIONAL PROTECTION <input checked="" type="checkbox"/>	RECOGNISED REFUGEES <input checked="" type="checkbox"/> PERSONS GRANTED INTERNATIONAL PROTECTION <input checked="" type="checkbox"/>	RECOGNISED REFUGEES <input checked="" type="checkbox"/> PERSONS GRANTED INTERNATIONAL PROTECTION <input checked="" type="checkbox"/>	
Article 12	Article 12	Article 12	
Blocking of data	Blocking of data	Blocking of data	
1. Data relating to an applicant for asylum	1. Data relating to an applicant for asylum	1. Data relating to an applicant for asylum	

<p>which have been recorded pursuant to Article 4(2) shall be blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member State of origin.</p>	<p>which have been recorded pursuant to Article 4(2) shall be blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member State of origin.</p>	<p>which have been recorded pursuant to Article 4(2) shall be blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member State of origin.</p>	
<p>As long as a decision pursuant to paragraph 2 has not been adopted, hits concerning persons who have been recognised and admitted as refugees in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.</p>	<p>As long as a decision pursuant to paragraph 2 has not been adopted, hits concerning persons who have been recognised and admitted as refugees in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.</p>	<p>As long as a decision pursuant to paragraph 2 has not been adopted, hits concerning persons who have been recognised and admitted as refugees in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.</p>	
<p>2. Five years after Eurodac starts operations, and on the basis of reliable statistics compiled by the Central Unit on persons who have lodged an application for asylum in a Member State after</p>	<p>2. Five years after Eurodac starts operations, and on the basis of reliable statistics compiled by the Central Unit on persons who have lodged an application for asylum in a Member State after</p>	<p>2. Five years after Eurodac starts operations, and on the basis of reliable statistics compiled by the Central Unit on persons who have lodged an application for asylum in a Member State after</p>	

<p>having been recognised and admitted as refugees in another Member State, a decision shall be taken in accordance with the relevant provisions of the Treaty, as to whether the data relating to persons who have been recognised and admitted as refugees in a Member State should:</p>	<p>having been recognised and admitted as refugees in another Member State, a decision shall be taken in accordance with the relevant provisions of the Treaty, as to whether the data relating to persons who have been recognised and admitted as refugees in a Member State should:</p>	<p>having been recognised and admitted as refugees in another Member State, a decision shall be taken in accordance with the relevant provisions of the Treaty, as to whether the data relating to persons who have been recognised and admitted as refugees in a Member State should:</p>	
<p>(a) be stored in accordance with Article 6 for the purpose of the comparison provided for in Article 4(3); or</p>	<p>(a) be stored in accordance with Article 6 for the purpose of the comparison provided for in Article 4(3); or</p>	<p>(a) be stored in accordance with Article 6 for the purpose of the comparison provided for in Article 4(3); or</p>	
<p>(b) be erased in advance once a person has been recognised and admitted as a refugee.</p>	<p>(b) be erased in advance once a person has been recognised and admitted as a refugee.</p>	<p>(b) be erased in advance once a person has been recognised and admitted as a refugee.</p>	
<p>3. In the case referred to in paragraph 2(a), the data blocked pursuant to paragraph 1 shall be unblocked and the procedure referred to in</p>	<p>3. In the case referred to in paragraph 2(a), the data blocked pursuant to paragraph 1 shall be unblocked and the procedure referred to in</p>	<p>3. In the case referred to in paragraph 2(a), the data blocked pursuant to paragraph 1 shall be unblocked and the procedure referred to in</p>	

paragraph 1 shall no longer apply.	paragraph 1 shall no longer apply.	paragraph 1 shall no longer apply.	
4. In the case referred to in paragraph 2(b):	4. In the case referred to in paragraph 2(b):	4. In the case referred to in paragraph 2(b):	
(a) data which have been blocked in accordance with paragraph 1 shall be erased immediately by the Central Unit; and	(a) data which have been blocked in accordance with paragraph 1 shall be erased immediately by the Central Unit; and	(a) data which have been blocked in accordance with paragraph 1 shall be erased immediately by the Central Unit; and	
(b) data relating to persons who are subsequently recognised and admitted as refugees shall be erased in accordance with Article 15(3), as soon as the Member State of origin becomes aware that the person has been recognised and admitted as a refugee in a Member State.	(b) data relating to persons who are subsequently recognised and admitted as refugees shall be erased in accordance with Article 15(3), as soon as the Member State of origin becomes aware that the person has been recognised and admitted as a refugee in a Member State.	(b) data relating to persons who are subsequently recognised and admitted as refugees shall be erased in accordance with Article 15(3), as soon as the Member State of origin becomes aware that the person has been recognised and admitted as a refugee in a Member State.	

<p>5. The implementing rules concerning the procedure for the blocking of data referred to in paragraph 1 and the compilation of statistics referred to in paragraph 2 shall be adopted in accordance with the procedure laid down in Article 22(1).</p>	<p>5. The implementing rules concerning the procedure for the blocking of data referred to in paragraph 1 and the compilation of statistics referred to in paragraph 2 shall be adopted in accordance with the procedure laid down in Article 22(1).</p>	<p>5. The implementing rules concerning the procedure for the blocking of data referred to in paragraph 1 and the compilation of statistics referred to in paragraph 2 shall be adopted in accordance with the procedure laid down in Article 22(1).</p>	
<p>Article 18 Marking of data</p>	<p>Article 18 Blocking of data</p>	<p>Article 18 Marking of data</p>	
<p>1. The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance</p>	<p>1. <i>Data relating to an applicant for international protection which have been recorded pursuant to Article 11 shall be blocked in the central database if that person is granted international protection in a Member State. Such blocking shall be carried out by the Central System on the instructions of the Member State of origin.</i></p>	<p>1. The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance</p>	<p>EP confirmed that it could accept the marking of data for asylum purposes, but not for law-enforcement purposes; its compromise for the entire Article is as follows:</p> <p>1. The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the</p>

<p>with Article 12 for the purpose of transmission under Article 9(5).</p>		<p>with Article 12 for the purpose of transmission under Article 9(5).</p>	<p>Central System in accordance with Article 12 for the purpose of transmission under Article 9(5).</p> <p>2. The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC).</p> <p><i>2a. <u>For the purposes as laid down in Article 1(2), hits concerning persons who have been granted international protection in a Member State shall not be transmitted. The Central System shall return a negative result to the requesting Member State.</u></i></p> <p>By way of compromise, the EP has suggested making the data under this Article available to law-enforcing authorities for a three-year period, which is in line with the duration of the residence permit granted to beneficiaries of international protection, under the</p>
--	--	--	---

			<p>Qualification Directive.</p> <p>The Cion has suggested the following compromise wording (maintaining two options regarding the time the relevant data should be made available for law enforcement purposes) (in bold underline and square brackets):</p> <p>1. For the purposes laid down in Article 1(1), the Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5). <u>The Central System shall inform all Member States of origin about the marking of data by another Member State of origin having produced a hit with data which they transmitted relating</u></p>
--	--	--	--

		<p><u>to persons referred to in Article 9(1) or Article 14(1). Those Member States of origin shall also mark the corresponding data sets.</u></p> <p><u>2. Data of beneficiaries of international protection stored in the Central System and marked pursuant to paragraph 1 shall be made available for comparison for the purposes laid down in Article 1(2) for a period of</u></p> <p style="padding-left: 40px;"><u>[five years after the data were first recorded in the Central System pursuant to Article 9(1).]</u></p> <p style="padding-left: 40px;"><u>[three years after the date on which the data subject was granted international protection].</u></p> <p><u>Where there is a hit, the Central System shall transmit for all the data sets corresponding to the hit the data referred to in Articles 11(a) to (k). The Central System shall not transmit the mark referred to in paragraph 1. Upon the expiry of the period of [five years / three</u></p>
--	--	--

		<p><u>years], the Central System shall automatically block such data from being transmitted in the case of a request for comparison for the purposes laid down in Article 1(2), whilst leaving these data available for comparison for the purpose laid down in Article 1(1) until the point of their erasure. Blocked data shall not be transmitted and the Central System shall return a negative result to the requesting Member State in the case of a hit.</u></p> <p><u>3</u> (former para. 2) The Member State of origin shall unmark <u>or unblock</u> data concerning a third country national or stateless person whose data were previously marked <u>or blocked</u> in accordance with paragraphs <u>1 or 2</u> if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive <u>2004/83/EC 2011/95/EU</u>.</p> <p>The Pres recommends to make the data available for law-</p>
--	--	--

			enforcement authorities for a five-year period, after the data were first recorded in the Central System pursuant to Article 9(1). with regard to working out an overall compromise.
2. The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.	2. <i>Hits concerning persons who have been granted international protection in a Member State shall not be transmitted. The Central System shall return a negative result to the requesting Member State.</i>	2. The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.	see above, under paragraph 1.

<p style="text-align: center;">CHAPTER VI</p>	<p style="text-align: center;">CHAPTER VI</p>	<p style="text-align: center;">CHAPTER VI</p>	
<p style="text-align: center;">PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES</p>	<p style="text-align: center;">PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES</p>	<p style="text-align: center;">PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES</p>	
<p style="text-align: center;"><i>Article 19</i> Procedure for comparison of fingerprint data with EURODAC data</p>	<p style="text-align: center;"><i>Article 19</i> Procedure for comparison of fingerprint data with EURODAC data</p>	<p style="text-align: center;"><i>Article 19</i> Procedure for comparison of fingerprint data with EURODAC data</p>	
<p>1. The designated authorities referred to in Article 5(1) and Europol may submit a reasoned electronic request to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying</p>	<p>1. The designated authorities referred to in Article 5(1) and Europol may submit a reasoned electronic request <i>as provided for in Article 20(1)</i> to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point.</p>	<p>1. <u>↻ For the purposes as laid down in Article 1 (2) the ☹ ↻ [...] ☹ designated authorities referred to in Article 5(1) and ↻ the designated authority of ☹ Europol ↻ referred to in Article 7(2) ☹ may submit a reasoned electronic request ↻ together with the reference number used by that authority's</u></p>	<p>The EP accepted the Council text with the addition of the reference to Art. 20(1):</p> <p>1. <u>↻ For the purposes as laid down in Article 1 (2) the ☹ ↻ [...] ☹ designated authorities referred to in Article 5(1) and ↻ the designated authority of ☹ Europol ↻ referred to in Article 7(2) ☹ may submit a reasoned</u></p>

<p>authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.</p>	<p>Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.</p>	<p><u>Member State or Europol,</u> ☒ to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.</p>	<p>electronic request <i>as provided for in Article 20(1)</i> ☒ <u>together with the reference number used by that authority's Member State or Europol,</u> ☒ to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.</p> <p>The compromise is agreed.</p>
<p>2. Where all the conditions for requesting a comparison are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the EURODAC Central System for the purpose of comparison with all the EURODAC data.</p>	<p>2. Where all the conditions for requesting a comparison are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the EURODAC Central System for the purpose of comparison with all the EURODAC data.</p>	<p>2. Where all the conditions for requesting a comparison are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the EURODAC Central System ☒ <u>according to the procedures laid down in Article 9 (3) and (5)</u> ☒ for the purpose of comparison with ☒ [...] ☒ the ☒ [...] ☒</p>	<p>EP accepted the Council text</p>

		data transmitted to the Central System pursuant to Article 9(1) and 14(2).	
3. In exceptional cases of urgency, 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 of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.	3. In exceptional cases of urgency <i>of the need to prevent an imminent danger associated with a terrorist or other serious criminal offence</i> , 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 of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.	3. In exceptional cases of urgency, 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 of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.	EP maintains its wish to insert its amendment in the text. Pres: recommends acceptance of the EP amendment
4. Where the ex-post verification determines that the access was not	4. Where the ex-post verification determines that the access was not	4. Where the ex-post verification determines that the access was not	Identical

<p>justified, the information communicated from EURODAC shall be destroyed by all authorities that have accessed it and they shall inform the verifying authority of such destruction.</p>	<p>justified, the information communicated from EURODAC shall be destroyed by all authorities that have accessed it and they shall inform the verifying authority of such destruction.</p>	<p>justified, the information communicated from EURODAC shall be destroyed by all authorities that have accessed it and they shall inform the verifying authority of such destruction.</p>	
	<p>4a. <i>The Commission shall publish an indicative, non-binding model EURODAC request form for use under this Article, which correctly reflects the criteria set out in Article 20(1).</i></p>		<p>In order to avoid any possible trespassing of the Commission's right of initiative, the Commissioner will volunteer to say in the EP Plenary that the Commission will propose an official Commission Recommendation, subject to consultation with the Member States and the EP, containing an indicative non-binding format to request access for law enforcement authorities to Eurodac</p> <p>Commission suggestion accepted</p>

<p style="text-align: center;"><i>Article 20</i></p> <p style="text-align: center;">Conditions for access to EURODAC data by designated authorities</p>	<p style="text-align: center;"><i>Article 20</i></p> <p style="text-align: center;">Conditions for access to EURODAC data by designated authorities</p>	<p style="text-align: center;"><i>Article 20</i></p> <p style="text-align: center;">Conditions for access to EURODAC data by designated authorities</p>	
<p>1. Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA return negative results and where:</p>	<p>1. Designated authorities may <i>submit a reasoned electronic request for</i> the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases, of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA <i>and of the Visa Information System when possible</i> return negative results and where <i>all the following cumulative conditions are met:</i></p>	<p>1. <u>☞ For the purposes as laid down in Article 1 (2) designated ☞ [...] ☞ authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA ☞ [...] ☞ did not lead to the establishment of the identity of the data subject ☞ and where:</u></p>	<p>The Pres strongly recommends the following compromise, with regard to working out an overall compromise:</p> <p>☞ <u>For the purposes as laid down in Article 1 (2) designated ☞ [...] ☞ authorities may submit a reasoned electronic request for the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons with the following data bases did not lead to the establishment of the identity of the data subject:</u></p> <ul style="list-style-type: none"> - national fingerprint databases, - the Automated Fingerprint Databases of all other Member States under Decision 2008/615/JHA where comparisons are technically available, unless there are reasonable grounds to believe

			<p><u>that the comparison</u> with such databases 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 sent by the designated authority to the verifying authority <u>and</u></p> <p><u>- the Visa Information System under Decision 2009/633/JHA provided that the conditions for such a comparison laid down in that Decision are met;</u></p> <p>and where the following cumulative conditions are met:</p>
<p>(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;</p>	<p>(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;</p>	<p>(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;</p>	<p>As a result of the third informal trilogue, the following compromise has been provisionally agreed upon by EP and Pres:</p> <p>(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences, <i>which means that there is an overriding public security concern which makes the querying of the database proportionate</i>".</p>

			The Pres recommends acceptance, with regard to working out an overall compromise
(b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and	(b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and	(b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and	Identical
(c) there are reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question.	(c) there <i>is an overriding public security concern which makes the querying of the database proportionate, and there are</i> reasonable grounds to consider that such comparison with EURODAC data will <i>substantially</i> contribute to the prevention, detection or investigation of any of the criminal	(c) there are reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question.	As a result of the third informal trilogue, the following compromise has been provisionally agreed upon by EP and Pres: (c) there are reasonable grounds to consider that such comparison with EURODAC data will <i>substantially</i> contribute to the prevention, detection or investigation of any of the criminal offences in question. <i><u>These reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist or other serious criminal offence falls in a category</u></i>

	offences in question.		<i>covered by this Regulation.</i> The Pres recommends acceptance with regard to working out an overall compromise
	<i>(ca) there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist or other serious criminal offence has applied for international protection.</i>		see under (c)
2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.	2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.	2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.	Identical
<i>Article 21</i> Conditions for access to EURODAC data by Europol	<i>Article 21</i> Conditions for access to EURODAC data by Europol	<i>Article 21</i> Conditions for access to EURODAC data by Europol	
1. Requests for comparison	1. Requests for comparison	1. [...] For the	EP compromise suggestion:

<p>with EURODAC data by Europol shall take place within the limits of its mandate and where necessary for the performance of its tasks pursuant to the Europol Decision and for the purposes of a specific analysis or an analysis of a general nature and of a strategic type.</p>	<p>with EURODAC data by Europol shall take place within the limits of its mandate and where necessary for the performance of its tasks pursuant to Decision 2009/371/JHA [...].</p>	<p>purposes as laid down in Article 1 (2) the designated authority of Europol may request the comparison of fingerprint data with those stored in the EURODAC central database within the limits of the mandate of Europol and where necessary for the performance of tasks of Europol only if comparisons with fingerprint data stored in any information processing system established at Europol did not lead to the establishment of the identity of the data subject and where</p>	<p>1. For the purposes as laid down in Article 1 (2) the designated authority of Europol may request the comparison of fingerprint data with those stored in the EURODAC central database within the limits of the mandate of Europol and where necessary for the performance of tasks of Europol only if comparisons with fingerprint data stored in any information processing</p> <p><i>new compromise suggestion:</i> <u>systems that are technically and legally accessible by EUROPOL</u>, did not lead to the establishment of the identity of the data subject and where (compromise suggestion accepted by EP and Council)</p> <p>It has been accepted to maintain points (a) to (c) adapted accordingly to the modifications which will be agreed upon in Art. 20(1) points (a) to (c) - see below.</p>
---	---	---	--

	<p><i>1a. However, access to EURODAC data by Europol shall be allowed only in specific cases, under specific circumstances and under the strict conditions provided for in Article 20(1).</i></p>		<p>EP agreed to the deletion of its compromise</p>
		<p>➔ (a) the comparison is necessary to support and strengthen action by Member States in preventing, detecting and investigating terrorist offences or other serious criminal offences falling under Europol's mandate; ☒</p>	<p>(a) the comparison is necessary to support and strengthen action by Member States in preventing, detecting and or investigating terrorist offences or other serious criminal offences falling under Europol's mandate, <i>which means that there is an overriding public security concern which makes the querying of the database proportionate</i>".</p> <p>The Pres recommends acceptance with regard to working out an overall compromise</p>
		<p>➔ (b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and ☒</p>	<p>Identical</p>

		<p>➔ (c) there are reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question. Ⓢ</p>	<p>(c) there are reasonable grounds to consider that such comparison with EURODAC data will <i>substantially</i> contribute to the prevention, detection or investigation of any of the criminal offences in question. <i><u>These reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist or other serious criminal offence falls in a category covered by this Regulation.</u></i></p> <p>The Pres recommends acceptance with regard to working out an overall compromise</p>
2. Requests for comparison with EURODAC data shall be limited to comparisons of fingerprint data.	2. Requests for comparison with EURODAC data shall be limited to comparisons of fingerprint data.	2. Requests for comparison with EURODAC data shall be limited to comparisons of fingerprint data.	Identical
3. Processing of information obtained by Europol from comparison with EURODAC shall be subject to the authorisation of the	3. Processing of information obtained by Europol from comparison with EURODAC shall be subject to the authorisation of the	3. Processing of information obtained by Europol from comparison with EURODAC shall be subject to the authorisation of the	Identical

Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.	Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.	Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.	
<i>Article 22</i> Communication between the verifying authorities and the National Access Points	<i>Article 22</i> Communication between the verifying authorities and the National Access Points	<i>Article 22</i> Communication between the designated authorities, the verifying authorities and the National Access Points	Council text accepted
1. EURODAC Communication Infrastructure shall be used for the data transmission by the verifying authorities of Member States and Europol to the National Access Points and vice versa. All communications shall take place electronically.	1. EURODAC Communication Infrastructure shall be used for the data transmission by the verifying authorities of Member States and Europol to the National Access Points and vice versa. All communications shall take place electronically.	1. [...] In accordance with Article 26, all communication between the designated authorities, the verifying authorities and the National Access points shall be secure and take place electronically.	Pres suggests replacing "In accordance with Art. 26..." with "without prejudice to Art. 26". EP agrees with the Pres suggestion
2. Fingerprints shall be digitally processed by the Member State and transmitted in the data format referred to in Annex I, in order to ensure that the	2. Fingerprints shall be digitally processed by the Member State and transmitted in the data format referred to in Annex I, in order to ensure that the	2. For the purposes as laid down in Article 1 (2) fingerprints [...] shall be digitally processed by the Member State and transmitted in the data format referred	Technical amendment - Council text agreed

comparison can be carried out by means of the computerised fingerprint recognition system.	comparison can be carried out by means of the computerised fingerprint recognition system.	to in Annex I, in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.	
CHAPTER VI VII	CHAPTER VI VII	CHAPTER VI VII	
<u>DATA PROCESSING USE</u>, DATA PROTECTION AND LIABILITY	<u>DATA PROCESSING USE</u>, DATA PROTECTION AND LIABILITY	<u>DATA PROCESSING USE</u>, DATA PROTECTION AND LIABILITY	
<i>Article 23 13</i> Responsibility for data processing use	<i>Article 23 13</i> Responsibility for data processing use	<i>Article 23 13</i> Responsibility for data processing use	Identical
1. The Member State of origin shall be responsible for ensuring that:	1. The Member State of origin shall be responsible for ensuring that:	1. The Member State of origin shall be responsible for ensuring that:	
(a) fingerprints are taken lawfully;	(a) fingerprints are taken lawfully;	(a) fingerprints are taken lawfully;	

<p>(b) fingerprint data and the other data referred to in Article 5(1) 11, Article 8(2) 14(2) and Article 11(2) 17(2) are lawfully transmitted to the Central Unit ⇒ System ⇐;</p>	<p>(b) fingerprint data and the other data referred to in Article 5(1) 11, Article 8(2) 14(2) and Article 11(2) 17(2) are lawfully transmitted to the Central Unit ⇒ System ⇐;</p>	<p>(b) fingerprint data and the other data referred to in Article 5(1) 11, Article 8(2) 14(2) and Article 11(2) 17(2) are lawfully transmitted to the Central Unit ⇒ System ⇐;</p>	
<p>(c) data are accurate and up-to-date when they are transmitted to the Central Unit ⇒ System ⇐;</p>	<p>(c) data are accurate and up-to-date when they are transmitted to the Central Unit ⇒ System ⇐;</p>	<p>(c) data are accurate and up-to-date when they are transmitted to the Central Unit ⇒ System ⇐;</p>	
<p>(d) without prejudice to the responsibilities of the Commission ⇒ Agency ⇐, data in the central database ⇒ Central System ⇐ are lawfully recorded, stored, corrected and erased;</p>	<p>(d) without prejudice to the responsibilities of the Commission ⇒ Agency ⇐, data in the central database ⇒ Central System ⇐ are lawfully recorded, stored, corrected and erased;</p>	<p>(d) without prejudice to the responsibilities of the Commission ⇒ Agency ⇐, data in the central database ⇒ Central System ⇐ are lawfully recorded, stored, corrected and erased;</p>	
<p>(e) the results of fingerprint data comparisons transmitted by the</p>	<p>(e) the results of fingerprint data comparisons transmitted by the</p>	<p>(e) the results of fingerprint data comparisons transmitted by the</p>	

<p>Central Unit ⇒ System ⇐ are lawfully <u>processed</u> <u>used</u>.</p>	<p>Central Unit ⇒ System ⇐ are lawfully <u>processed</u> <u>used</u>.</p>	<p>Central Unit ⇒ System ⇐ are lawfully <u>processed</u> <u>used</u>.</p>	
<p>2. In accordance with Article 14 <u>34</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 Unit ⇒ System ⇐ as well as the security of the data it receives from the Central Unit ⇒ System ⇐.</p>	<p>2. In accordance with Article 14 <u>34</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 Unit ⇒ System ⇐ as well as the security of the data it receives from the Central Unit ⇒ System ⇐.</p>	<p>2. In accordance with Article 14 <u>34</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 Unit ⇒ System ⇐ as well as the security of the data it receives from the Central Unit ⇒ System ⇐.</p>	
<p>3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article 4(6) <u>25(4)</u>.</p>	<p>3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article 4(6) <u>25(4)</u>.</p>	<p>3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article 4(6) <u>25(4)</u>.</p>	
<p>4. The Commission ⇒ Agency ⇐ shall ensure that the Central Unit ⇒ System ⇐ is operated in accordance with the provisions of this Regulation and its implementing rules. In</p>	<p>4. The Commission ⇒ Agency ⇐ shall ensure that the Central Unit ⇒ System ⇐ is operated in accordance with the provisions of this Regulation and its implementing rules. In</p>	<p>4. The Commission ⇒ Agency ⇐ shall ensure that the Central Unit ⇒ System ⇐ is operated in accordance with the provisions of this Regulation and its implementing rules. In</p>	

<p>particular, the Commission ⇒ Agency ⇐ shall:</p>	<p>particular, the Commission ⇒ Agency ⇐ shall:</p>	<p>particular, the Commission ⇒ Agency ⇐ shall:</p>	
<p>(a) adopt measures ensuring that persons working ⇒ with ⇐ in the Central Unit ⇒ System ⇐ process use the data recorded ⊗ therein ⊗ in the central database only in accordance with the purpose of EurodacEURODA <u>C</u> as laid down in Article 1(1);</p>	<p>(a) adopt measures ensuring that persons working ⇒ with ⇐ in the Central Unit ⇒ System ⇐ process use the data recorded ⊗ therein ⊗ in the central database only in accordance with the purpose of EurodacEURODA <u>C</u> as laid down in Article 1(1);</p>	<p>(a) adopt measures ensuring that persons working ⇒ with ⇐ in the Central Unit ⇒ System ⇐ process use the data recorded ⊗ therein ⊗ in the central database only in accordance with the purpose of EurodacEURODA <u>C</u> as laid down in Article 1(1);</p>	
<p>(b) ensure that persons working in the Central System comply with all requests from Member States made pursuant to this Regulation in relation to recording, comparison, correction and erasure of data for</p>	<p>(b) ensure that persons working in the Central System comply with all requests from Member States made pursuant to this Regulation in relation to recording, comparison, correction and erasure of data for</p>	<p>(b) ensure that persons working in the Central System comply with all requests from Member States made pursuant to this Regulation in relation to recording, comparison, correction and erasure of data for</p>	

<p>which they are responsible;</p>	<p>which they are responsible;</p>	<p>which they are responsible;</p>	
<p>(b) (e) take the necessary measures to ensure the security of the Central Unit ⇒ System ⇐ in accordance with Article 14 34;</p>	<p>(b) (e) take the necessary measures to ensure the security of the Central Unit ⇒ System ⇐ in accordance with Article 14 34;</p>	<p>(b) (e) take the necessary measures to ensure the security of the Central Unit ⇒ System ⇐ in accordance with Article 14 34;</p>	
<p>(c) (d) ensure that only persons authorised to work ⇒ with ⇐ in the Central Unit ⇒ System ⇐ have access ⊗ thereto ⊗ to data recorded in the central database, without prejudice to Article 20 and the powers of the independent supervisory body which will be established under Article 286(2) of the Treaty ⊗ the competences of the European Data Protection</p>	<p>(c) (d) ensure that only persons authorised to work ⇒ with ⇐ in the Central Unit ⇒ System ⇐ have access ⊗ thereto ⊗ to data recorded in the central database, without prejudice to Article 20 and the powers of the independent supervisory body which will be established under Article 286(2) of the Treaty ⊗ the competences of the European Data Protection</p>	<p>(c) (d) ensure that only persons authorised to work ⇒ with ⇐ in the Central Unit ⇒ System ⇐ have access ⊗ thereto ⊗ to data recorded in the central database, without prejudice to Article 20 and the powers of the independent supervisory body which will be established under Article 286(2) of the Treaty ⊗ the competences of the European Data Protection</p>	

Supervisor ☒ .	Supervisor ☒ .	Supervisor ☒ .	
The Commission ⇒ Agency ⇐ shall inform the European Parliament and the Council ⇒ as well as the European Data Protection Supervisor ⇐ of the measures it takes pursuant to the first subparagraph.	The Commission ⇒ Agency ⇐ shall inform the European Parliament and the Council ⇒ as well as the European Data Protection Supervisor ⇐ of the measures it takes pursuant to the first subparagraph.	The Commission ⇒ Agency ⇐ shall inform the European Parliament and the Council ⇒ as well as the European Data Protection Supervisor ⇐ of the measures it takes pursuant to the first subparagraph.	
<i>Article 24 2</i> Transmission	<i>Article 24 2</i> Transmission	<i>Article 24 2</i> Transmission	
1. Fingerprints shall be digitally processed and transmitted in the data format referred to in Annex I. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐, the Central Unit ☒ Agency ☒ shall establish the technical requirements for transmission of the data format by Member States to the Central Unit ⇒ System ⇐ and vice	1. Fingerprints shall be digitally processed and transmitted in the data format referred to in Annex I. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐, the Central Unit ☒ Agency ☒ shall establish the technical requirements for transmission of the data format by Member States to the Central Unit ⇒ System ⇐ and vice	1. Fingerprints shall be digitally processed and transmitted in the data format referred to in Annex I. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐, the Central Unit ☒ Agency ☒ shall establish the technical requirements for transmission of the data format by Member States to the Central Unit ⇒ System ⇐ and vice	Identical

<p>versa. The Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall ensure that the fingerprint data transmitted by the Member States can be compared by the computerised fingerprint recognition system.</p>	<p>versa. The Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall ensure that the fingerprint data transmitted by the Member States can be compared by the computerised fingerprint recognition system.</p>	<p>versa. The Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall ensure that the fingerprint data transmitted by the Member States can be compared by the computerised fingerprint recognition system.</p>	
<p>2. Member States should <input checked="" type="checkbox"/> shall <input checked="" type="checkbox"/> transmit the data referred to in Article 5(1) 11(1), Article 14(2) and Article 17(2) of the Eurodac Regulation electronically. <input checked="" type="checkbox"/> The data referred to in Article 11(1) and Article 14(2) shall be automatically recorded in the Central System. <input checked="" type="checkbox"/> As far as it is necessary for the efficient operation of the Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/>, the Central Unit <input checked="" type="checkbox"/> Agency <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 Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> and vice</p>	<p>2. Member States should <input checked="" type="checkbox"/> shall <input checked="" type="checkbox"/> transmit the data referred to in Article 5(1) 11(1), Article 14(2) and Article 17(2) of the Eurodac Regulation electronically. <input checked="" type="checkbox"/> The data referred to in Article 11(1) and Article 14(2) shall be automatically recorded in the Central System. <input checked="" type="checkbox"/> As far as it is necessary for the efficient operation of the Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/>, the Central Unit <input checked="" type="checkbox"/> Agency <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 Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> and vice</p>	<p>2. Member States should <input checked="" type="checkbox"/> shall <input checked="" type="checkbox"/> transmit the data referred to in Article 5(1) 11(1), Article 14(2) and Article 17(2) of the Eurodac Regulation electronically. <input checked="" type="checkbox"/> The data referred to in Article 11(1) and Article 14(2) shall be automatically recorded in the Central System. <input checked="" type="checkbox"/> As far as it is necessary for the efficient operation of the Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/>, the Central Unit <input checked="" type="checkbox"/> Agency <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 Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> and vice</p>	<p>Identical</p>

<p>versa. Transmission of data in paper form using the form set out in Annex II or by other means of data support (diskettes, CD-ROM or other means of data support which may be developed and generally used in future) should be limited to situations in which there are continuous technical problems.</p>	<p>versa. Transmission of data in paper form using the form set out in Annex II or by other means of data support (diskettes, CD-ROM or other means of data support which may be developed and generally used in future) should be limited to situations in which there are continuous technical problems.</p>	<p>versa. Transmission of data in paper form using the form set out in Annex II or by other means of data support (diskettes, CD-ROM or other means of data support which may be developed and generally used in future) should be limited to situations in which there are continuous technical problems.</p>	
<p>3. The reference number referred to in Article 5(1)(d) <u>11(d)</u> and Article 14(2)(d) and 17(1) of the Eurodac Regulation 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 an asylum seeker or a person referred to in Article 8 or Article 11 of the Eurodac Regulation <u>9</u>, Article 14 or Article 17.</p>	<p>3. The reference number referred to in Article 5(1)(d) <u>11(d)</u> and Article 14(2)(d) and 17(1) of the Eurodac Regulation 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 an asylum seeker or a person referred to in Article 8 or Article 11 of the Eurodac Regulation <u>9</u>, Article 14 or Article 17.</p>	<p>3. The reference number referred to in ... <u>Articles 11(d), 14(2)(d) and 17(1) and 19 (1) of the Eurodac Regulation</u> 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 an asylum seeker or a person referred to in Article 8 or Article 11 of the Eurodac</p>	<p>Technical amendment agreed</p>

		<u>Regulation 9, Article 14 or Article 17.</u>	
<p><u>4.</u> The reference number shall begin with the identification letter or letters by which, in accordance with the norm referred to in Annex I, the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person. "1" refers to data relating to asylum seekers ☒ persons referred to in Article 9(1) ☒, "2" to persons referred to in Article § 14(1) of the Eurodac Regulation and "3" to persons referred to in Article 11 17 of the Eurodac Regulation.</p>	<p><u>4.</u> The reference number shall begin with the identification letter or letters by which, in accordance with the norm referred to in Annex I, the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person. "1" refers to data relating to asylum seekers ☒ persons referred to in Article 9(1) ☒, "2" to persons referred to in Article § 14(1) of the Eurodac Regulation and "3" to persons referred to in Article 11 17 of the Eurodac Regulation.</p>	<p><u>4.</u> The reference number shall begin with the identification letter or letters by which, in accordance with the norm referred to in Annex I, the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person or request ☒ . "1" refers to data relating to asylum seekers ☒ persons referred to in Article 9(1) ☒, "2" to persons referred to in Article § 14(1) ☒, ☒ of the Eurodac Regulation ☒ [...] ☒ "3" to persons referred to in Article 11 17 ☒, "4" to requests referred to in Article 20, and "5" to requests referred to in Article 21 and "9" to requests referred to in article 29 ☒ of the Eurodac</p>	<p>Technical amendment agreed</p>

		<u>Regulation.</u>	
5. The Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> .	5. The Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> .	5. The Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> .	Identical
64. The Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> shall confirm receipt of the transmitted data as soon as possible. To this end the Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.	64. The Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> shall confirm receipt of the transmitted data as soon as possible. To this end the Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.	64. The Central Unit <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> shall confirm receipt of the transmitted data as soon as possible. To this end the Central Unit <input checked="" type="checkbox"/> Agency <input checked="" type="checkbox"/> shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.	Identical
<i>Article 25 3</i> Carrying out comparisons and transmitting results	<i>Article 25 3</i> Carrying out comparisons and transmitting results	<i>Article 25 3</i> Carrying out comparisons and transmitting results	
1. Member States shall ensure the transmission of fingerprint data in an appropriate quality for	1. Member States shall ensure the transmission of fingerprint data in an appropriate quality for	1. Member States shall ensure the transmission of fingerprint data in an appropriate quality for	Identical

<p>the purpose of comparison by means of the computerised fingerprint recognition system. As far as it is necessary to ensure that the results of the comparison by the Central Unit</p> <p>⇒ System ⇐ reach a very high level of accuracy, the Central Unit</p> <p>⇒ Agency ⇐ shall define the appropriate quality of transmitted fingerprint data. The Central Unit</p> <p>⇒ System ⇐ shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data do not lend themselves to comparison using the computerised fingerprint recognition system, the Central Unit</p> <p>⇒ System ⇐ shall, as soon as possible,</p> <p>⇒ inform ⇐ the Member State. ⇒ The Member State concerned shall ⇐ transmit fingerprint data of the appropriate quality</p>	<p>the purpose of comparison by means of the computerised fingerprint recognition system. As far as it is necessary to ensure that the results of the comparison by the Central Unit</p> <p>⇒ System ⇐ reach a very high level of accuracy, the Central Unit</p> <p>⇒ Agency ⇐ shall define the appropriate quality of transmitted fingerprint data. The Central Unit</p> <p>⇒ System ⇐ shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data do not lend themselves to comparison using the computerised fingerprint recognition system, the Central Unit</p> <p>⇒ System ⇐ shall, as soon as possible,</p> <p>⇒ inform ⇐ the Member State. ⇒ The Member State concerned shall ⇐ transmit fingerprint data of the appropriate quality</p>	<p>the purpose of comparison by means of the computerised fingerprint recognition system. As far as it is necessary to ensure that the results of the comparison by the Central Unit</p> <p>⇒ System ⇐ reach a very high level of accuracy, the Central Unit</p> <p>⇒ Agency ⇐ shall define the appropriate quality of transmitted fingerprint data. The Central Unit</p> <p>⇒ System ⇐ shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data do not lend themselves to comparison using the computerised fingerprint recognition system, the Central Unit</p> <p>⇒ System ⇐ shall, as soon as possible,</p> <p>⇒ inform ⇐ the Member State. ⇒ The Member State concerned shall ⇐ transmit fingerprint data of the appropriate quality</p>	
--	--	--	--

<p>⇒ using the same reference number of the previous set of fingerprint data ⇐.</p>	<p>⇒ using the same reference number of the previous set of fingerprint data ⇐.</p>	<p>⇒ using the same reference number of the previous set of fingerprint data ⇐.</p>	
<p>2. The Central Unit ⇐ System ⇐ shall carry out comparisons in the order of arrival of requests. Each request must be dealt with within 24 hours. In the case of data which are transmitted electronically, <u>at</u> <u>A</u> Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where these times cannot be respected owing to circumstances which are outside the Central Unit ⇐ Agency's ⇐ responsibility, the Central Unit ⇐ System ⇐ shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as it is</p>	<p>2. The Central Unit ⇐ System ⇐ shall carry out comparisons in the order of arrival of requests. Each request must be dealt with within 24 hours. In the case of data which are transmitted electronically, <u>at</u> <u>A</u> Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where these times cannot be respected owing to circumstances which are outside the Central Unit ⇐ Agency's ⇐ responsibility, the Central Unit ⇐ System ⇐ shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as it is</p>	<p>2. The Central Unit ⇐ System ⇐ shall carry out comparisons in the order of arrival of requests. Each request must be dealt with within 24 hours. In the case of data which are transmitted electronically, <u>at</u> <u>A</u> Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where these times cannot be respected owing to circumstances which are outside the Central Unit ⇐ Agency's ⇐ responsibility, the Central Unit ⇐ System ⇐ shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as it is</p>	<p>Identical</p>

<p>necessary for the efficient operation of the Central Unit ⇒ System ⇐ , the Central Unit ⇒ Agency ⇐ shall establish criteria to ensure the priority handling of requests.</p>	<p>necessary for the efficient operation of the Central Unit ⇒ System ⇐ , the Central Unit ⇒ Agency ⇐ shall establish criteria to ensure the priority handling of requests.</p>	<p>necessary for the efficient operation of the Central Unit ⇒ System ⇐ , the Central Unit ⇒ Agency ⇐ shall establish criteria to ensure the priority handling of requests.</p>	
<p>3. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐ , the Central Unit ⇒ Agency ⇐ shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.</p>	<p>3. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐ , the Central Unit ⇒ Agency ⇐ shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.</p>	<p>3. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐ , the Central Unit ⇒ Agency ⇐ shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.</p>	Identical
<p><u>4.</u> The results of the comparison shall be immediately checked in the Member State of origin ⇒ by a fingerprint expert ⇐. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to</p>	<p>4. The results of the comparison shall be immediately checked in the Member State of origin by a <i>trained</i> fingerprint expert. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to</p>	<p><u>4.</u> The results of the comparison shall be immediately checked in the receiving Member State ⇒ [...] ⇐ ⇒ by a fingerprint expert as defined in accordance with its national rules, specifically trained in the types of fingerprint comparisons included in</p>	Council amendments agreed by the EP

<p>Article 15 32 of the Dublin Convention ⊗ Regulation ⊗.</p>	<p>Article 32 of Regulation (EU) No [...] of the European Parliament and of the Council of ... [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]*.</p>	<p>this Regulation ⊗ ⊗ . ⊗ For the purposes as laid down in Article 1 (1), final ⊗ ⊗ [...] ⊗ identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to Article 15 32 of the Dublin Convention ⊗ Regulation ⊗.</p>	<p>Technical - reference should be made to Art. 34 of the Dublin Regulation</p>
<p>Information received from the Central Unit ⊗ System ⊗ relating to other data found to be unreliable shall be erased or destroyed as soon as the unreliability of the data is established.</p>	<p>Information received from the Central Unit ⊗ System ⊗ relating to other data found to be unreliable shall be erased or destroyed as soon as the unreliability of the data is established.</p>	<p>Information received from the Central Unit ⊗ System ⊗ relating to other data found to be unreliable shall be erased or destroyed as soon as the unreliability of the data is established.</p>	
<p>5. Where final identification in accordance with paragraph 4 reveal that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the</p>	<p>5. Where final identification in accordance with paragraph 4 reveals that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact <i>as soon as</i></p>	<p>5. Where final identification in accordance with paragraph 4 reveal that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the</p>	<p>As a result of the third informal trilogue the Cion compromise to replace the 72-hour deadline of the EP amendment, with three working days, is provisionally</p>

<p>Commission and to the Agency.</p>	<p><i>possible and no later than after 72 hours</i> to the Commission and to the Agency. <i>The Central System shall transmit a maximum of the five best matching fingerprints to the designated authorities referred to in Article 5(1) and Europol.</i></p>	<p>Commission and to the Agency.</p>	<p>agreed by EP and Council.</p> <p>EP amendment (on five best matching fingerprints) to be further considered by the EP. The Council cannot accept this amendment, on the basis of technical and legal considerations.</p> <p>Cion pointed out that it prefers no restriction on the number of fingerprints.</p>
<p><i>Article 26 4</i> Communication between Member States and the Central Unit ⇔ System ⇔</p>	<p><i>Article 26 4</i> Communication between Member States and the Central Unit ⇔ System ⇔</p>	<p><i>Article 26 4</i> Communication between Member States and the Central Unit ⇔ System ⇔</p>	<p>Identical</p>
<p>Data transmitted from the Member States to the Central Unit ⇔ System ⇔ and vice versa shall use IDA generic services referred to in Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on a series of</p>	<p>Data transmitted from the Member States to the Central Unit ⇔ System ⇔ and vice versa shall use IDA generic services referred to in Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on a series of</p>	<p>Data transmitted from the Member States to the Central Unit ⇔ System ⇔ and vice versa shall use IDA generic services referred to in Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on a series of</p>	

<p>guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA) ⇒ the EURODAC Communication Infrastructure ⇐. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐, the Central Unit ⊗ Agency ⊗ shall establish the technical procedures necessary for the use of IDA-generic services ⇒ the Communication ⇐.</p>	<p>guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA) ⇒ the EURODAC Communication Infrastructure ⇐. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐, the Central Unit ⊗ Agency ⊗ shall establish the technical procedures necessary for the use of IDA-generic services ⇒ the Communication ⇐.</p>	<p>guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA) ⇒ the EURODAC Communication Infrastructure ⇐. As far as it is necessary for the efficient operation of the Central Unit ⇒ System ⇐, the Central Unit ⊗ Agency ⊗ shall establish the technical procedures necessary for the use of IDA-generic services ⇒ the Communication ⇐.</p>	
<p>Article 14 Security</p>	<p>Article 14 Security</p>	<p>Article 14 Security</p>	
<p>1. The Member State of origin shall take the necessary measures to:</p>	<p>1. The Member State of origin shall take the necessary measures to:</p>	<p>1. The Member State of origin shall take the necessary measures to:</p>	

<p>(a) prevent any unauthorised person from having access to national installations in which the Member State carries out operations in accordance with the aim of Eurodae (checks at the entrance to the installation);</p>	<p>(a) prevent any unauthorised person from having access to national installations in which the Member State carries out operations in accordance with the aim of Eurodae (checks at the entrance to the installation);</p>	<p>(a) prevent any unauthorised person from having access to national installations in which the Member State carries out operations in accordance with the aim of Eurodae (checks at the entrance to the installation);</p>	
<p>(b) prevent data and data media in Eurodae from being read, copied, modified or erased by unauthorised persons (control of data media);</p>	<p>(b) prevent data and data media in Eurodae from being read, copied, modified or erased by unauthorised persons (control of data media);</p>	<p>(b) prevent data and data media in Eurodae from being read, copied, modified or erased by unauthorised persons (control of data media);</p>	
<p>(c) guarantee that it is possible to check and establish a posteriori what data have been recorded in Eurodae when and by whom (control of data recording);</p>	<p>(c) guarantee that it is possible to check and establish a posteriori what data have been recorded in Eurodae when and by whom (control of data recording);</p>	<p>(c) guarantee that it is possible to check and establish a posteriori what data have been recorded in Eurodae when and by whom (control of data recording);</p>	




<p>(d) prevent the unauthorised recording of data in Eurodac and any unauthorised modification or erasure of data recorded in Eurodac (control of data entry);</p>	<p>(d) prevent the unauthorised recording of data in Eurodac and any unauthorised modification or erasure of data recorded in Eurodac (control of data entry);</p>	<p>(d) prevent the unauthorised recording of data in Eurodac and any unauthorised modification or erasure of data recorded in Eurodac (control of data entry);</p>	
<p>(e) guarantee that, in using Eurodac, authorised persons have access only to data which are within their competence (control of access);</p>	<p>(e) guarantee that, in using Eurodac, authorised persons have access only to data which are within their competence (control of access);</p>	<p>(e) guarantee that, in using Eurodac, authorised persons have access only to data which are within their competence (control of access);</p>	
<p>(f) guarantee that it is possible to check and establish to which authorities data recorded in Eurodac may be transmitted by data transmission equipment (control of transmission);</p>	<p>(f) guarantee that it is possible to check and establish to which authorities data recorded in Eurodac may be transmitted by data transmission equipment (control of transmission);</p>	<p>(f) guarantee that it is possible to check and establish to which authorities data recorded in Eurodac may be transmitted by data transmission equipment (control of transmission);</p>	
<p>(g) prevent the unauthorised</p>	<p>(g) prevent the unauthorised</p>	<p>(g) prevent the unauthorised</p>	

<p>reading, copying, modification or erasure of data during both the direct transmission of data to or from the central database and the transport of data media to or from the Central Unit (control of transport).</p>	<p>reading, copying, modification or erasure of data during both the direct transmission of data to or from the central database and the transport of data media to or from the Central Unit (control of transport).</p>	<p>reading, copying, modification or erasure of data during both the direct transmission of data to or from the central database and the transport of data media to or from the Central Unit (control of transport).</p>	
<p>2. As regards the operation of the Central Unit, the Commission shall be responsible for applying the measures mentioned under paragraph 1.</p>	<p>2. As regards the operation of the Central Unit, the Commission shall be responsible for applying the measures mentioned under paragraph 1.</p>	<p>2. As regards the operation of the Central Unit, the Commission shall be responsible for applying the measures mentioned under paragraph 1.</p>	
<p><i>Article 27 45</i> Access to, and correction or erasure of, data recorded in EurodacEURODAC</p>	<p><i>Article 27 45</i> Access to, and correction or erasure of, data recorded in EurodacEURODAC</p>	<p><i>Article 27 45</i> Access to, and correction or erasure of, data recorded in EurodacEURODAC</p>	
<p>1. The Member State of origin shall have access to data which it has transmitted and which are recorded in the central database ⇒ Central System ⇐ in accordance</p>	<p>1. The Member State of origin shall have access to data which it has transmitted and which are recorded in the central database ⇒ Central System ⇐ in accordance</p>	<p>1. The Member State of origin shall have access to data which it has transmitted and which are recorded in the central database ⇒ Central System ⇐ in accordance</p>	<p>Identical</p>

with the provisions of this Regulation.	with the provisions of this Regulation.	with the provisions of this Regulation.	
No Member State may conduct searches in the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in Article 4(5) 9(5).	No Member State may conduct searches in the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in Article 4(5) 9(5).	No Member State may conduct searches in the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in Article 4(5) 9(5).	
<p>2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the central database ⇒ Central System ⇐ shall be those designated by each Member State ⇒ for the purpose of Article 1(1). This 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</p>	<p>2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the Central System shall be those designated by each Member State for the purpose of Article 1(1). That designation shall specify the <i>precise</i> unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and the Agency a list of those</p>	<p>2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the central database ⇒ Central System ⇐ shall be those designated by each Member State ⇒ for the purpose of Article 1(1). This 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</p>	<p>The agreed compromise reads as follows: That designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation.</p> <p>The EP amendment regarding the use of the word "units" is agreed.</p>

<p>Agency ⇐ a list of those authorities ⇒ and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish once a year an updated consolidated list. ⇐</p>	<p><i>units</i> and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish once a year an updated consolidated list <i>online</i>.</p>	<p>Agency ⇐ a list of those authorities ⇒ and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish once a year an updated consolidated list. ⇐</p>	<p>Technical - accepted as the OJ is already available online</p>
<p>3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central Unit ⇐ System ⇐ by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article 6, Article 10(1) or Article 12(4)(a) 12 or Article 16(1).</p>	<p>3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central Unit ⇐ System ⇐ by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article 6, Article 10(1) or Article 12(4)(a) 12 or Article 16(1).</p>	<p>3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central Unit ⇐ System ⇐ by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article 6, Article 10(1) or Article 12(4)(a) 12 or Article 16(1).</p>	<p>Identical</p> <p>Technical - reference should be made only to para. 2 of Art. 12 (this Art. will have two numbered paragraphs).</p>
<p>Where the Member State of origin records data directly in the central database, it may amend</p>	<p>Where the Member State of origin records data directly in the central database, it may amend</p>	<p>Where the Member State of origin records data directly in the central database, it may amend</p>	

or erase the data directly.	or erase the data directly.	or erase the data directly.	
Where the Member State of origin does not record data directly in the central database, the Central Unit shall amend or erase the data at the request of that Member State.	Where the Member State of origin does not record data directly in the central database, the Central Unit shall amend or erase the data at the request of that Member State.	Where the Member State of origin does not record data directly in the central database, the Central Unit shall amend or erase the data at the request of that Member State.	
4. If a Member State or the Central Unit ⇒ Agency ⇐ has evidence to suggest that data recorded in the central database ⇒ Central System ⇐ are factually inaccurate, it shall advise the Member State of origin as soon as possible.	4. If a Member State or the Central Unit ⇒ Agency ⇐ has evidence to suggest that data recorded in the central database ⇒ Central System ⇐ are factually inaccurate, it shall advise the Member State of origin as soon as possible.	4. If a Member State or the Central Unit ⇒ Agency ⇐ has evidence to suggest that data recorded in the central database ⇒ Central System ⇐ are factually inaccurate, it shall advise the Member State of origin as soon as possible.	Identical

<p>If a Member State has evidence to suggest that data were recorded in the central database ⇒ Central System ⇐ contrary to this Regulation, it shall similarly advise ⇒ the Agency, the Commission and ⇐ the Member State of origin as soon as possible. The latter shall check the data concerned and, if necessary, amend or erase them without delay.</p>	<p>If a Member State has evidence to suggest that data were recorded in the central database ⇒ Central System ⇐ contrary to this Regulation, it shall similarly advise ⇒ the Agency, the Commission and ⇐ the Member State of origin as soon as possible. The latter shall check the data concerned and, if necessary, amend or erase them without delay.</p>	<p>If a Member State has evidence to suggest that data were recorded in the central database ⇒ Central System ⇐ contrary to this Regulation, it shall similarly advise ⇒ the Agency, the Commission and ⇐ the Member State of origin as soon as possible. The latter shall check the data concerned and, if necessary, amend or erase them without delay.</p>	
<p>5. The Central Unit ⇒ Agency ⇐ shall not transfer or make available to the authorities of any third country data recorded in the central database ⇒ Central System ⇐, unless it is specifically authorised to do so in the framework of a Community agreement on the criteria and mechanisms for determining the State responsible for examining an application</p>	<p>5. The Central Unit ⇒ Agency ⇐ shall not transfer or make available to the authorities of any third country data recorded in the central database ⇒ Central System ⇐, unless it is specifically authorised to do so in the framework of a <i>Union</i> agreement on the criteria and mechanisms for determining the State responsible for examining an application</p>	<p>5. The Central Unit ⇒ Agency ⇐ shall not transfer or make available to the authorities of any third country data recorded in the central database ⇒ Central System ⇐, unless it is specifically authorised to do so in the framework of a  [...]  <u>Union</u>  agreement on the criteria and mechanisms for determining the State responsible for examining an application</p>	<p>Identical</p> <p>Technical - agreed to have reference to the "Dublin Regulation".</p>

for asylum ⇒ international protection ⇐ .	for asylum ⇒ international protection ⇐ .	for asylum ⇒ international protection ⇐ .	
Article 22	Article 22	Article 22	
Implementing rules	Implementing rules	Implementing rules	
1. The Council shall adopt, acting by the majority laid down in Article 205(2) of the Treaty, the implementing provisions necessary for	1. The Council shall adopt, acting by the majority laid down in Article 205(2) of the Treaty, the implementing provisions necessary for	1. The Council shall adopt, acting by the majority laid down in Article 205(2) of the Treaty, the implementing provisions necessary for	
laying down the procedure referred to in Article 4(7),	laying down the procedure referred to in Article 4(7),	laying down the procedure referred to in Article 4(7),	
laying down the procedure for the blocking of the data referred to in Article 12(1),	laying down the procedure for the blocking of the data referred to in Article 12(1),	laying down the procedure for the blocking of the data referred to in Article 12(1),	
drawing up the statistics referred to in Article 12(2).	drawing up the statistics referred to in Article 12(2).	drawing up the statistics referred to in Article 12(2).	

<p>In cases where these implementing provisions have implications for the operational expenses to be borne by the Member States, the Council shall act unanimously.</p>	<p>In cases where these implementing provisions have implications for the operational expenses to be borne by the Member States, the Council shall act unanimously.</p>	<p>In cases where these implementing provisions have implications for the operational expenses to be borne by the Member States, the Council shall act unanimously.</p>	
<p>2. The measures referred to in Article 3(4) shall be adopted in accordance with the procedure referred to in Article 23(2).</p>	<p>2. The measures referred to in Article 3(4) shall be adopted in accordance with the procedure referred to in Article 23(2).</p>	<p>2. The measures referred to in Article 3(4) shall be adopted in accordance with the procedure referred to in Article 23(2).</p>	
<p><i>Article 28 16</i> Keeping of records by the Central Unit</p>	<p><i>Article 28 16</i> Keeping of records by the Central Unit</p>	<p><i>Article 28 16</i> Keeping of records by the Central Unit</p>	
<p>1. The Central Unit ⇒ Agency ⇐ shall keep records of all data processing operations within the Central Unit ⇒ System ⇐. These records shall show the purpose of access, the date and time, the data transmitted, the data used for interrogation and the name of both the unit putting ☒ entering ☒ in</p>	<p>1. The Central Unit ⇒ Agency ⇐ shall keep records of all data processing operations within the Central Unit ⇒ System ⇐. These records shall show the purpose of access, the date and time, the data transmitted, the data used for interrogation and the name of both the unit putting ☒ entering ☒ in</p>	<p>1. The Central Unit ⇒ Agency ⇐ shall keep records of all data processing operations within the Central Unit ⇒ System ⇐. These records shall show the purpose of access, the date and time, the data transmitted, the data used for interrogation and the name of both the unit putting ☒ entering ☒ in</p>	<p>Identical</p>

<p>or retrieving the data and the persons responsible.</p>	<p>or retrieving the data and the persons responsible.</p>	<p>or retrieving the data and the persons responsible.</p>	
<p>2. Such records 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 14 34. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year ⇒ after the retention period referred to in Article 12 and in Article 16(1) has expired ⇐, if they are not required for monitoring procedures which have already begun.</p>	<p>2. Such records 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 14 34. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year ⇒ after the retention period referred to in Article 12 and in Article 16(1) has expired ⇐, if they are not required for monitoring procedures which have already begun.</p>	<p>2. Such records 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 14 34. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year ⇒ after the retention period referred to in Article 12 and in Article 16(1) has expired ⇐, if they are not required for monitoring procedures which have already begun.</p>	<p>Identical</p> <p>Technical - reference should be made only to para. 1 of Art. 12 (this Art. will have two numbered paragraphs).</p>
<p>3. Each Member State shall take the necessary measures in order to achieve the objectives set out in paragraph 1 and 2 in relation to its national system. In addition, each Member State shall keep records of the staff duly</p>	<p>3. Each Member State shall take the necessary measures in order to achieve the objectives set out in paragraph 1 and 2 in relation to its national system. In addition, each Member State shall keep records of the staff duly</p>	<p>3. ⇒ For the purposes as laid down in Article 1 (1) each ◉ ⇒ [...] ◉ Member State shall take the necessary measures in order to achieve the objectives set out in paragraph 1 and 2 in relation to its national</p>	<p>Technical amendment - Council text agreed</p>

authorised to enter or retrieve the data.	authorised to enter or retrieve the data.	system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.	
Article 23	Article 23	Article 23	
Committee	Committee	Committee	
1. The Commission shall be assisted by a committee.	1. The Commission shall be assisted by a committee.	1. The Commission shall be assisted by a committee.	
2. In the cases where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply.	2. In the cases where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply.	2. In the cases where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply.	
The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.	The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.	The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.	
3. The committee shall adopt its rules of procedure.	3. The committee shall adopt its rules of procedure.	3. The committee shall adopt its rules of procedure.	

<p style="text-align: center;"><i>Article 29 18</i> Rights of the data subject</p>	<p style="text-align: center;"><i>Article 29 18</i> Rights of the data subject</p>	<p style="text-align: center;"><i>Article 29 18</i> Rights of the data subject</p>	
<p>1. A person covered by this Regulation shall be informed by the Member State of origin \Rightarrow in writing, and where appropriate, orally, in a language which he or she understands or may reasonably be presumed to understand \Leftarrow of the following:</p>	<p>1. A person covered by this Regulation shall be informed by the Member State of origin in writing, and where <i>necessary</i>, orally, in a language <i>that</i> he or she understands or <i>is</i> reasonably <i>supposed</i> to understand of the following:</p>	<p>1. A person covered by ... \Rightarrow <u>Article 9, Article 14 and Article 17</u> \Leftarrow shall be informed by the Member State of origin \Rightarrow in writing, and where appropriate, orally, in a language which he or she understands or may reasonably be presumed to understand \Leftarrow of the following:</p>	<p>Both EP and Council amendments are accepted; the compromise text reads as follows:</p> <p>"A person covered by Article 9, Article 14 and Article 17 shall be informed by the Member State of origin in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand of the following:"</p>
<p>(a) the identity of the controller and of his representative, if any;</p>	<p>(a) the identity of the controller and of his representative, if any;</p>	<p>(a) the identity of the controller and of his representative, if any;</p>	
<p>(b) the \boxtimes regarding \boxtimes the purpose for which the \boxtimes his or her \boxtimes data will be processed within EurodacEURODA <u>C</u> \Rightarrow including a description of the aims of the Dublin</p>	<p>(b) regarding the purpose for which his or her data will be processed within EURODAC including a description of the aims of the Dublin Regulation, in</p>	<p>(b) the \boxtimes regarding \boxtimes the purpose for which the \boxtimes his or her \boxtimes data will be processed within EurodacEURODA <u>C</u> \Rightarrow including a description of the aims of the Dublin</p>	<p>As a result of the third informal trilogue, EP and Council have provisionally agreed to the following compromise:</p> <p>"(b) regarding the purpose for which his or her data will be processed within EURODAC including a description of the aims of the Dublin Regulation, in</p>

Regulation, in accordance with Article 4 of that Regulation ↵.	accordance with Article 4 of that Regulation <i>and a comprehensive explanation of the fact that EURODAC may be accessed by the Member States and Europol for law enforcement purposes.</i>	Regulation, in accordance with Article 4 of that Regulation ↵.	accordance with Article 4 of that Regulation <i>and an comprehensive explanation of the fact that EURODAC may be accessed by the Member States and Europol for law enforcement purposes, in an intelligible form, using clear and plain language, <u>adapted to the data subject</u>''</i>
(c) the recipients of the data;	(c) the recipients of the data;	(c) the recipients of the data;	Identical
(d) in relation to a person covered by Article 4 9 or Article 8 14 , the obligation to have his/her fingerprints taken;	(d) in relation to a person covered by Article 4 9 or Article 8 14 , the obligation to have his/her fingerprints taken;	(d) in relation to a person covered by Article 4 9 or Article 8 14 , the obligation to have his/her fingerprints taken;	Identical
(e) the existence of the right of access to and the right to rectify, the data <input checked="" type="checkbox"/> relating to him/her concerning him/her <input checked="" type="checkbox"/> , and the right to request that inaccurate data	(e) the [...] right of access to data relating to him/her, and the right to request that inaccurate data relating to him/her be corrected or that unlawfully	(e) the existence of the right of access to and the right to rectify, the data <input checked="" type="checkbox"/> relating to him/her concerning him/her <input checked="" type="checkbox"/> , and the right to request that inaccurate data	EP amendment accepted by Council

<p>relating to him/her be corrected ☒ ⇒ or ██████ that unlawfully ██████ processed data relating to them be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the ██████ National Supervisory Authorities referred to in Article 31(1) ⇐.</p>	<p>processed data relating to <i>him/her</i> be erased, as well as the [...] procedures for exercising those rights including the contact details of the controller and the ██████ National Supervisory Authorities referred to in Article 31(1).</p>	<p>relating to him/her be corrected ☒ ⇒ or ██████ that unlawfully ██████ processed data relating to ██████ [...] ⇐ ⇒ <u>him/her</u> ⇐ be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the ██████ National Supervisory Authorities referred to in Article 31(1) ⇐.</p>	<p>EP amendment accepted by Council</p> <p>Technical - reference should be made to Art. 30(1).</p>
<p>In relation to a person covered by Article <u>4 9</u> or Article <u>8 14</u>, the information referred to in the first subparagraph shall be provided when his/her fingerprints are taken.</p>	<p>In relation to a person covered by Article <u>4 9</u> or Article <u>8 14</u>, the information referred to in the first subparagraph shall be provided when his/her fingerprints are taken.</p>	<p>In relation to a person covered by Article <u>4 9</u> or Article <u>8 14</u>, the information referred to in the first subparagraph shall be provided when his/her fingerprints are taken.</p>	

<p>In relation to a person covered by Article 11 17, the information referred to in the first subparagraph shall be provided no later than the time when the data relating to the person are transmitted to the Central Unit ⇨ System ⇩. This obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.</p>	<p>In relation to a person covered by Article 11 17, the information referred to in the first subparagraph shall be provided no later than the time when the data relating to the person are transmitted to the Central Unit ⇨ System ⇩. This obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.</p>	<p>In relation to a person covered by Article 11 17, the information referred to in the first subparagraph shall be provided no later than the time when the data relating to the person are transmitted to the Central Unit ⇨ System ⇩. This obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.</p>	
<p>A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 4(1) of the Dublin Regulation shall be drawn up in accordance with the procedure referred to in Article 40(2) of the Dublin Regulation. The leaflet should be "clear and simple, drafted in a language that the person</p>	<p>A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 4(1) of Regulation (EU) No [...] of the European Parliament and of the Council of ... [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international</p>	<p>A common leaflet, containing ⇨ [...] ⇩ the ⇨ relevant ⇩ information referred to in paragraph 1 of this Article and the information referred to in Article 4(⇨ 1 ⇩ ⇨ [...] ⇩ ⇨ [...] ⇩) of the Dublin Regulation shall be drawn up in accordance with the procedure referred to in Article 40(2) of the Dublin Regulation. The leaflet should be</p>	<p>As a result of the third informal trilogue the following compromise has been provisionally agreed between EP and Council:</p> <p>"A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 4(1) of Regulation (EU) No [...] of the European Parliament and of the Council of ... [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for</p>

<p>understands or may reasonably be presumed to understand.</p>	<p><i>protection lodged in one of the Member States by a third-country national or a stateless person]* shall be drawn up in accordance with the procedure referred to in Article 40(2) of Regulation [.../...]*. The leaflet shall be "clear and simple, drafted in a language that the person understands or is reasonably supposed to understand". It shall also include information on the rights of the data subject and the possibility of assistance by the National Supervisory Authorities as well as the contact details of the controller and the National Supervisory Authorities.</i></p>	<p>☞ [...]. ☺ clear and simple, drafted in a language that the person understands or may reasonably be presumed to understand.</p>	<p><i>international protection lodged in one of the Member States by a third-country national or a stateless person]* shall be drawn up in accordance with the procedure referred to in Article 40(2) (Technical: reference should be made instead to Art. 44(2)) of Regulation [.../...]*. The leaflet shall be clear and simple, drafted in a language that the person understands or is reasonably supposed to understand. The leaflet shall be established in such a manner as to enable Member States to complete it with additional Member State-specific information. This Member State-specific information shall include at least the rights of the data subject, the possibility of assistance by the National Supervisory Authorities, as well as the contact details of the office of the controller and the National Supervisory Authorities".</i></p>
---	--	--	--

<p>Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner.</p>	<p>Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner. <i>The Commission shall provide templates of the leaflets for adults and minors to the Member States. The best interests of the child shall be a primary consideration for the Member States when applying this Article.</i></p>	<p>Where a person covered by Article 9, Article 14 and Article 17 [...] is a minor, Member States shall provide the information in an age-appropriate manner.</p>	<p>Council technical amendments are accepted by the EP</p> <p>Deletion of the first sentence of the EP amendment is accepted by the EP</p> <p>EP insists on maintaining the second sentence of its amendment in the operative part of the Regulation.</p> <p>Pres recommends deletion of the second sentence as this concern is already covered by the new overarching Recital 27.</p>
<p>2. 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.</p>	<p>2. 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.</p>	<p>2. [...] For the purposes as laid down in Article 1 (1) 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.</p>	<p>Technical -Council text accepted</p>

<p>Without prejudice to the obligation to provide other information in accordance with point (a) of Article 12 of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him/her recorded in the central database ⇒ Central System ⇐ and of the Member State which transmitted them to the Central Unit ⇒ System ⇐. Such access to data may be granted only by a Member State.</p>	<p>Without prejudice to the obligation to provide other information in accordance with point (a) of Article 12 of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him/her recorded in the central database ⇒ Central System ⇐ and of the Member State which transmitted them to the Central Unit ⇒ System ⇐. Such access to data may be granted only by a Member State.</p>	<p>Without prejudice to the obligation to provide other information in accordance with point (a) of Article 12 of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him/her recorded in the central database ⇒ Central System ⇐ and of the Member State which transmitted them to the Central Unit ⇒ System ⇐. Such access to data may be granted only by a Member State.</p>	
<p>3. In each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be carried out without excessive delay by the Member State which transmitted the data, in</p>	<p>3. In each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be carried out without excessive delay by the Member State which transmitted the data, in</p>	<p>3. <u>⇒ For the purposes as laid down in Article 1 (1) in</u> ☉ <u>☉ [...]</u> ☉ each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be carried out without excessive delay</p>	<p>Technical - Council text accepted</p>

<p>accordance with its laws, regulations and procedures.</p>	<p>accordance with its laws, regulations and procedures.</p>	<p>by the Member State which transmitted the data, in accordance with its laws, regulations and procedures.</p>	
<p>4. If the rights of correction and erasure are exercised in a Member State, other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of the Member State, or States, in question so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the central database ⇒ Central System ⇐.</p>	<p>4. If the rights of correction and erasure are exercised in a Member State, other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of the Member State, or States, in question so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the central database ⇒ Central System ⇐.</p>	<p>4. <u>⇒ For the purposes as laid down in Article 1 (1) if ☉ ⇒ [...] ☉</u> the rights of correction and erasure are exercised in a Member State, other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of the Member State, or States, in question so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the central database ⇒ Central System ⇐.</p>	<p>Technical - Council text accepted</p>
<p>5. If it emerges that data recorded in the central database ⇒ Central System ⇐ are factually inaccurate or have been recorded unlawfully, the</p>	<p>5. If it emerges that data recorded in the central database ⇒ Central System ⇐ are factually inaccurate or have been recorded unlawfully, the</p>	<p>5. <u>⇒ For the purposes as laid down in Article 1 (1) if ☉ ⇒ [...] ☉</u> it emerges that data recorded in the central database ⇒ Central System ⇐ are</p>	<p>Technical – Council text accepted</p>

<p>Member State which transmitted them shall correct or erase the data in accordance with Article 15(3) 27(3). That Member State shall confirm in writing to the data subject without excessive delay that it has taken action to correct or erase data relating to him/her.</p>	<p>Member State which transmitted them shall correct or erase the data in accordance with Article 15(3) 27(3). That Member State shall confirm in writing to the data subject without excessive delay that it has taken action to correct or erase data relating to him/her.</p>	<p>factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall correct or erase the data in accordance with Article 15(3) 27(3). That Member State shall confirm in writing to the data subject without excessive delay that it has taken action to correct or erase data relating to him/her.</p>	
<p>6. If the Member State which transmitted the data does not agree that data recorded in the central database ⇒ 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.</p>	<p>6. If the Member State which transmitted the data does not agree that data recorded in the central database ⇒ 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.</p>	<p>6. ☞ For the purposes as laid down in Article 1 (1) if ☞ ☞ [...] ☞ the Member State which transmitted the data does not agree that data recorded in the central database ⇒ 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.</p>	<p>Technical – Council text accepted</p>

<p>That Member State shall also provide the data subject with information explaining the steps which he/she can take if he/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.</p>	<p>That Member State shall also provide the data subject with information explaining the steps which he/she can take if he/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.</p>	<p>That Member State shall also provide the data subject with information explaining the steps which he/she can take if he/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.</p>	
<p>7. Any request under paragraphs 2 and 3 shall contain all the necessary particulars to identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the rights referred to in paragraphs 2 and 3 and shall be destroyed</p>	<p>7. Any request under paragraphs 2 and 3 shall contain all the necessary particulars to identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the rights referred to in paragraphs 2 and 3 and shall be destroyed</p>	<p>7. Any request under paragraphs 2 and 3 shall contain all the necessary particulars to identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the rights referred to in paragraphs 2 and 3 and shall be destroyed</p>	<p>Identical</p>

immediately afterwards.	immediately afterwards.	immediately afterwards.	
8. The competent authorities of the Member States shall cooperate actively to enforce promptly the rights laid down in paragraphs 3, 4 and 5.	8. The competent authorities of the Member States shall cooperate actively to enforce promptly the rights laid down in paragraphs 3, 4 and 5.	8. The competent authorities of the Member States shall cooperate actively to enforce promptly the rights laid down in paragraphs 3, 4 and 5.	Identical
9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made, and shall make this document available to the National Supervisory Authorities without delay, upon their request.	9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made, and shall make this document available to the National Supervisory Authorities without delay, upon their request. <i>It shall immediately inform the National Supervisory Authorities when a person requests the correction or erasure of his or her data. No later than three weeks after the request, the competent authority shall confirm to the</i>	9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made, and shall make this document available to the National Supervisory Authorities without delay, upon their request.	As a result of the third informal trilogue the following compromise has been provisionally agreed upon by the EP and the Pres: 9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made <u>and how it was addressed</u> , and shall make this document available to the National Supervisory Authorities without delay, upon their request. (the rest of the EP amendment is deleted) The Pres recommends acceptance of the compromise as part of the overall compromise on the proposal.

	<p><i>National Supervisory Authorities that it has taken action to correct or erase the data or, where the Member State concerned does not agree that the data recorded in the Central System are inaccurate or have been recorded unlawfully, it shall explain why it is not prepared to correct or erase the data.</i></p>		
<p>9 10. In each Member State, the national supervisory authority shall ⇨ on the basis of his/her request, ⇨ assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his/her rights.</p>	<p>9 10. In each Member State, the national supervisory authority shall ⇨ on the basis of his/her request, ⇨ assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his/her rights.</p>	<p>9 10. ⇨ For the purposes as laid down in Article 1 (1) in ⇨ [...] ⇨ each Member State, the national supervisory authority shall ⇨ on the basis of his/her request, ⇨ assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his/her rights.</p>	Technical - Council text accepted
<p>10 11. The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of</p>	<p>10 11. The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of</p>	<p>10 11. ⇨ For the purposes as laid down in Article 1 (1) the ⇨ [...] ⇨ national supervisory authority of the Member State which</p>	Technical - Council text accepted

<p>the Member State in which the data subject is present shall assist and, where requested, advise him/her in exercising his/her right to correct or erase data. Both national supervisory authorities shall cooperate to this end. Requests for such assistance may be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data. The data subject may also apply for assistance and advice to the joint supervisory authority set up by Article 20.</p>	<p>the Member State in which the data subject is present shall assist and, where requested, advise him/her in exercising his/her right to correct or erase data. Both national supervisory authorities shall cooperate to this end. Requests for such assistance may be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data. The data subject may also apply for assistance and advice to the joint supervisory authority set up by Article 20.</p>	<p>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/her in exercising his/her right to correct or erase data. Both national supervisory authorities shall cooperate to this end. Requests for such assistance may be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data. The data subject may also apply for assistance and advice to the joint supervisory authority set up by Article 20.</p>	
<p>11. <u>12.</u> In each Member State any person may, in accordance with the laws, regulations and</p>	<p>11. <u>12.</u> In each Member State any person may, in accordance with the laws, regulations and</p>	<p>11. <u>12.</u> In each Member State any person may, in accordance with the laws, regulations and</p>	

<p>procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he/she is refused the right of access provided for in paragraph 2.</p>	<p>procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he/she is refused the right of access provided for in paragraph 2.</p>	<p>procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he/she is refused the right of access provided for in paragraph 2.</p>	
<p>12 <u>13</u>. 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/her recorded in the central database ⇒ Central System ⇐, in order to exercise his/her rights under paragraph 3. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject, in accordance with paragraph 10 <u>13</u> ,</p>	<p>12 <u>13</u>. 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/her recorded in the central database ⇒ Central System ⇐, in order to exercise his/her rights under paragraph 3. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject, in accordance with paragraph 10 <u>13</u> ,</p>	<p>12 <u>13</u>. 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/her recorded in the central database ⇒ Central System ⇐, in order to exercise his/her rights under paragraph 3. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject, in accordance with paragraph 10 <u>13</u> ,</p>	

<p>shall subsist throughout the proceedings.</p>	<p>shall subsist throughout the proceedings.</p>	<p>☞ [...]☞ ☞ 11☞ , shall subsist throughout the proceedings.</p>	<p>Technical - Council text accepted</p>
<p><i>Article 30 19</i> ☒ Supervision by the ☒ National <u>S</u>upervisory <u>A</u>uthority</p>	<p><i>Article 30 19</i> ☒ Supervision by the ☒ National <u>S</u>upervisory <u>A</u>uthority</p>	<p><i>Article 30 19</i> ☒ Supervision by the ☒ National <u>S</u>upervisory <u>A</u>uthority</p>	
<p>1. Each Member State shall provide that the national supervisory authority or authorities designated pursuant to Article 28(1) of Directive 95/46/EC shall monitor independently, in accordance with its respective national law, the lawfulness of the processing, in accordance with this Regulation, of personal data by the Member State in question, including their transmission to the Central Unit ☞ System ☞.</p>	<p>1. Each Member State shall provide that the national supervisory authority or authorities designated pursuant to Article 28(1) of Directive 95/46/EC shall monitor independently, in accordance with its respective national law, the lawfulness of the processing, in accordance with this Regulation, of personal data by the Member State in question, including their transmission to the Central Unit ☞ System ☞.</p>	<p>1. ☞ <u>For the purposes as laid down in Article 1 (1) each ☞</u> ☞ [...]☞ Member State shall provide that the national supervisory authority or authorities designated pursuant to Article 28(1) of Directive 95/46/EC shall monitor independently, in accordance with its respective national law, the lawfulness of the processing, in accordance with this Regulation, of personal data by the Member State in question, including their transmission to the Central Unit ☞ System ☞.</p>	<p>Technical - Council text accepted</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 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 fingerprint data.</p>	<p>Identical</p>
<p style="text-align: center;"><i>Article 31</i> Supervision by the European Data Protection Supervisor</p>	<p style="text-align: center;"><i>Article 31</i> Supervision by the European Data Protection Supervisor</p>	<p style="text-align: center;"><i>Article 31</i> Supervision by the European Data Protection Supervisor</p>	
<p>1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.</p>	<p>1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency <i>and by Europol</i> are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.</p>	<p>1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.</p>	<p>Council text accepted</p>
<p>2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with</p>	<p>2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with</p>	<p>2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with</p>	

<p>international auditing standards at least every four years. A report of such audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.</p>	<p>international auditing standards at least every <i>two years</i>. A report of such audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.</p>	<p>international auditing standards at least every four years. A report of such audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.</p>	<p>By way of compromise, Pres suggests that the audit should take place every three years. Compromise provisionally agreed</p>
<p><i>Article 32</i> Cooperation between National Supervisory Authorities and the European Data Protection Supervisor</p>	<p><i>Article 32</i> Cooperation between National Supervisory Authorities and the European Data Protection Supervisor</p>	<p><i>Article 32</i> Cooperation between National Supervisory Authorities and the European Data Protection Supervisor</p>	
<p>1. The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of EURODAC.</p>	<p>1. The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of EURODAC.</p>	<p>1. The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of EURODAC.</p>	<p>Identical</p>

	<p><i>1a. The National Supervisory Authority shall ensure that every year an audit of the processing of personal data in accordance with Article 1(2) is carried out, including an analysis of all reasoned electronic requests.</i></p>		<p>By way of compromise the EP suggests the following wording:</p> <p><i>The National Supervisory Authority shall ensure that every year an audit of the processing of personal data in accordance with Article 1(2) is carried out, including an analysis of reasoned electronic requests.</i></p> <p>The Pres suggests the following alternative compromise:</p> <p><i><u>Member States shall ensure that every year an audit of the processing of personal data in accordance with Article 1(2) is carried out, including an analysis of a sample of reasoned electronic requests.</u></i></p>
	<p><i>The audit shall be attached to the Member State annual report referred to in Article 40(8).</i></p>		
<p>2. They shall, each acting within the scope of its respective competences, exchange relevant</p>	<p>2. They shall, each acting within the scope of its respective competences, exchange relevant</p>	<p>2. They shall, each acting within the scope of its respective competences, exchange relevant</p>	<p>Identical</p>








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.	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.	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.	
	2a. Both the National and the European Supervisory Authorities shall be provided with sufficient financial and personal resources to be able adequately to supervise the use of and access to Eurodac data.		The Pres cannot accept the EP amendment as it is outside the scope of this Regulation
3. The National Supervisory Authorities and the European Data Protection Supervisor shall meet for	3. The National Supervisory Authorities and the European Data Protection Supervisor shall meet for	3. The National Supervisory Authorities and the European Data Protection Supervisor shall meet for	Identical

<p>that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Agency every two years.</p>	<p>that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Agency every two years.</p>	<p>that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Agency every two years.</p>	
<p><i>Article 33</i> Protection of personal data for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences</p>	<p><i>Article 33</i> Protection of personal data for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences</p>	<p><i>Article 33</i> Protection of personal data for the purposes of the prevention, detection and investigation of terrorist offences ... and of other serious criminal offences</p>	<p>Council can accept the EP text in consistency with Art. 6(1).</p>
<p>1. The Framework Decision 2008/977/JHA is applicable to the processing of relevant</p>	<p>1. The Framework Decision 2008/977/JHA is applicable to the processing of relevant</p>	<p>1. ... Each Member State shall provide that the provisions adopted under</p>	<p>Council technical amendment accepted by the EP</p>

<p>personal data for law enforcement purposes under this Regulation.</p>	<p>personal data for law enforcement purposes under this Regulation.</p>	<p>national law implementing Framework Decision 2008/977/JHA [...] are also applicable to the processing of [...] personal data by its national authorities for [...] the purposes as laid down in Article 1 (2) [...].</p>	<p>Technical - Council text agreed</p>
<p>2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA.</p>	<p>2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA.</p>	<p>2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA and shall be supervised by an independent external data protection supervisor. The provisions of that Decision in Article 30 on the individual's rights of access, Article 31 on the data subject's right to correction and deletion of data and Article 32 on appeals shall therefore be applicable to the processing of personal</p>	<p>Council amendment provisionally accepted by the EP</p>

		data by Europol pursuant to this Regulation; the independent external data protection supervisor shall ensure that the rights of the individual are not violated ☹.	
3. Personal data obtained pursuant to this Regulation from EURODAC shall only be processed for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences.	3. Personal data obtained pursuant to this Regulation from EURODAC <i>for the purposes as laid down in Article 1(2)</i> shall only be processed for the purposes of the prevention, detection and investigation of <i>the specific criminal investigation for which the data have been requested by that Member State, or Europol.</i>	3. Personal data obtained pursuant to this Regulation from EURODAC ☹ <u>for the purposes as laid down in Article 1 (2)</u> ☹ shall only be processed for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences.	<p>Cion suggested rewording the EP as follows: "... for the purposes of the prevention, detection or investigation of the specific criminal investigation case for which the data have been requested by that Member State, or Europol.</p> <p>Pres recommends acceptance of the EP compromise along with the Commission rewording.</p>
4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if	4. <i>The record of the search shall be kept by the Eurodac central system and the verifying authorities and Europol for the purpose of permitting the national data protection</i>	4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC ☹ <u>for the purposes as laid down in Article 1 (2)</u> ☹ shall be erased in national and	<p>Cion suggested including in the EP amendment a reference to designated authorities which shall keep records for the purposes of monitoring: "The record of the search shall be kept by the Eurodac central system, the responsible authorities and Europol for the</p>

<p>the data are not required for a specific ongoing criminal investigation by that Member State, or Europol.</p>	<p><i>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 draft the reports specified in Article 40(8). Other than for the above-mentioned purposes, personal data, as well as the record of the search, shall be erased in all national and Europol files after a period of one month, if the data are not required for the purposes of the specific ongoing criminal investigation for which the data have been requested by that Member State, or Europol.</i></p>	<p>Europol files after a period of one month, if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol.</p>	<p>purpose of..."</p> <p>The Pres recommends acceptance of the EP amendment with the Cion rewording.</p>
<p>5. The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States, including</p>	<p>5. The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States, including</p>	<p>5. The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States ➡ for the</p>	<p>Council amendment accepted by the EP. The provision is going to be transferred as a new paragraph, after paragraph 1 of the Article</p>

<p>their transmission to and from EURODAC shall be carried out by the national competent authorities designated pursuant to Framework Decision 2008/977/JHA.</p>	<p>their transmission to and from EURODAC shall be carried out by the national competent authorities designated pursuant to Framework Decision 2008/977/JHA.</p>	<p>purposes as laid down in Article 1 (2) , including their transmission to and from EURODAC shall be carried out by the national  [...]  supervisory  authorities designated pursuant to Framework Decision 2008/977/JHA.</p>	
<p>Article 34 Data security</p>	<p>Article 34 Data security</p>	<p>Article 34 Data security</p>	
<p>1. The Member State of origin shall ensure the security of the data before and during transmission to the Central System.</p>	<p>1. The Member State of origin shall ensure the security of the data before and during transmission to the Central System.</p>	<p>1. The Member State of origin shall ensure the security of the data before and during transmission to the Central System.</p>	Identical
<p>2. Each Member State shall, in relation to its national system, adopt the necessary measures, including a security plan, in order to:</p>	<p>2. Each Member State shall, in relation to its national system, adopt the necessary measures, including a security plan, in order to:</p>	<p>2. Each Member State shall, in relation to  [...]  all data processed by its relevant authorities pursuant to this Regulation, , adopt the necessary measures, including a security plan, in order to:</p>	EP accepted the Council amendment

<p>(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;</p>	<p>(a) physically protect data, including by making contingency plans for the protection of relevant infrastructure;</p>	<p>(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;</p>	<p>EP amendment to be considered by the Council and the EP</p>
<p>(b) deny unauthorised persons access to national installations in which the Member State carries out operations in accordance with the purpose of EURODAC (checks at entrance to the installation);</p>	<p>(b) deny unauthorised persons access to national installations in which the Member State carries out operations in accordance with the purpose of EURODAC (checks at entrance to the installation);</p>	<p>(b) deny unauthorised persons access to national installations in which the Member State carries out operations in accordance with the purpose of EURODAC (checks at entrance to the installation);</p>	<p>Identical</p>
<p>(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);</p>	<p>(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);</p>	<p>(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);</p>	<p>Identical</p>
<p>(d) prevent the unauthorised input of data and the unauthorised</p>	<p>(d) prevent the unauthorised input of data and the unauthorised</p>	<p>(d) prevent the unauthorised input of data and the unauthorised</p>	<p>Identical</p>

inspection, modification or erasure of stored personal data (storage control);	inspection, modification or erasure of stored personal data (storage control);	inspection, modification or erasure of stored personal data (storage control);	
(e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or erasure of data processed in EURODAC (control of data entry);	(e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or erasure of data processed in EURODAC (control of data entry);	(e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or erasure of data processed in EURODAC (control of data entry);	Identical
(f) ensure that persons authorised to access EURODAC have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);	(f) ensure that persons authorised to access EURODAC have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);	(f) ensure that persons authorised to access EURODAC have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);	Identical

<p>(g) ensure that all authorities with a right of access to EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 25 of Framework Decision 2008/977/JHA without delay at their request (personnel profiles);</p>	<p>(g) ensure that all authorities with a right of access to EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data and make these profiles and any other relevant information which the authorities may require for the purpose of carrying out supervision available to the National Supervisory Authorities referred to in Article 28 of Directive 95/46/EC and in Article 25 of Framework Decision 2008/977/JHA without delay at their request</p>	<p>(g) ensure that all authorities with a right of access to EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 25 of Framework Decision 2008/977/JHA without delay at their request (personnel profiles);</p>	<p>EP amendment accepted</p>
--	---	--	------------------------------

	(personnel profiles);		
(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);	(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);	(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);	Identical
(i) ensure that it is possible to verify and establish what data have been processed in EURODAC, when, by whom and for what purpose (control of data recording);	(i) ensure that it is possible to verify and establish what data have been processed in EURODAC, when, by whom and for what purpose (control of data recording);	(i) ensure that it is possible to verify and establish what data have been processed in EURODAC, when, by whom and for what purpose (control of data recording);	Identical
(j) prevent the unauthorised reading, copying, modification or erasure of personal data during the transmission of	(j) prevent the unauthorised reading, copying, modification or erasure of personal data during the transmission of	(j) prevent the unauthorised reading, copying, modification or erasure of personal data during the transmission of	Identical

<p>personal data to or from EURODAC or during the transport of data media, in particular by means of appropriate encryption techniques (transport control);</p>	<p>personal data to or from EURODAC or during the transport of data media, in particular by means of appropriate encryption techniques (transport control);</p>	<p>personal data to or from EURODAC or during the transport of data media, in particular by means of appropriate encryption techniques (transport control);</p>	
<p>(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).</p>	<p>(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing) and also near real-time observation of the system using specialized tools. Member States shall inform the Agency of the security incidents detected on their</p>	<p>(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).</p>	<p>As regards the first sentence of the EP amendment, by way of compromise, the Cion suggests the following wording (in bold, underline):</p> <p>"monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures</p>

	<p><i>system. The Agency shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents. All parties shall collaborate during a security incident.</i></p>		<p>related to internal monitoring to ensure compliance with this Regulation (self-auditing) <u>and to automatically detect within 24 hours any relevant events arising in the application of measures listed in subparagraphs (b) to (j) that might indicate a security incident.</u></p> <p>The Pres recommends acceptance of this Cion compromise.</p> <p>For the second sentence of the EP amendment (starting from "Member States shall inform the agency...", the Pres recommends acceptance.</p> <p>As a result of the third informal trilogue the last sentence of the EP amendment has been provisionally agreed to read: "The Member States concerned, the Agency and Europol shall collaborate during a security incident".</p>
<p>3. The Agency shall take the necessary measures in order to achieve the objectives set out in</p>	<p>3. The Agency shall take the necessary measures in order to achieve the objectives set out in</p>	<p>3. The Agency shall take the necessary measures in order to achieve the objectives set out in</p>	<p>Identical</p>

paragraph 2 as regards the operation of EURODAC, including the adoption of a security plan.	paragraph 2 as regards the operation of EURODAC, including the adoption of a security plan.	paragraph 2 as regards the operation of EURODAC, including the adoption of a security plan.	
Article 35 Prohibition of transfers of data to third countries or to international bodies or to private parties	Article 35 Prohibition of transfers of data to third countries or to international bodies or to private parties	Article 35 Prohibition of transfers of data to third countries or to international bodies or to private parties	
Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.	Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. <i>Personal data obtained by a Member State or Europol and processed further in national databases shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the Union.</i> This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the	Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.	As a result of the third informal trilogue EP and Pres have agreed to test the following wording: Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database, <u>as well as such data subsequently further processed at national level,</u> shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.

	Dublin Regulation applies.		<p>The Presidency suggests the following alternative wording:</p> <ol style="list-style-type: none"> 1. Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC Central System shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall also apply if these data are further processed at national level or between Member States within the meaning of Article 2(b) of Council Framework Decision 2008/977/JHA. 2. Personal data which originated in a Member State and are exchanged between Member States subsequent to a hit received for the purpose of Article 1(2) shall not be transferred to third countries if there is a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of fundamental rights.
--	----------------------------	--	---

			<p>3. The prohibitions referred to in paragraphs 1 and 2 shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.</p> <p>The Pres recommends acceptance of its alternative wording with regard to working out an overall compromise.</p> <p>·</p> <p>See also comments under Recital 33</p>
<p><i>Article 36</i> Logging and documentation</p>	<p><i>Article 36</i> Logging and documentation</p>	<p><i>Article 36</i> Logging and documentation</p>	
<p>1. Each Member Stat and Europol shall ensure that all data processing operations resulting from requests for comparison with EURODAC data pursuant to this Regulation are logged or documented for the purposes of checking the admissibility of the request monitoring the lawfulness of the data</p>	<p>1. Each Member Stat and Europol shall ensure that all data processing operations resulting from requests for comparison with EURODAC data pursuant to this Regulation are logged or documented for the purposes of checking the admissibility of the request monitoring the lawfulness of the data</p>	<p>1. Each Member ... State and Europol shall ensure that all data processing operations resulting from requests for comparison with EURODAC data ... for the purposes as laid down in Article 1 (2) are logged or documented for the purposes of checking the admissibility of the</p>	<p>Council amendment accepted by the EP</p>

processing and data integrity and security and for self-monitoring.	processing and data integrity and security and for self-monitoring.	request monitoring the lawfulness of the data processing and data integrity and security and for self-monitoring.	
2. The log or documentation shall show in all cases:	2. The log or documentation shall show in all cases:	2. The log or documentation shall show in all cases:	Identical
(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;	(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;	(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;	
			In relation with the provisional compromise reached in Art. 20(1), EP and Pres suggest the following addition: (aa) the reasonable grounds given not to conduct comparison with other Member States under Council Decision 2008/615/JHA, in accordance with Article 20(1).

(b) the respective national file reference;	(b) the respective national file reference;	(b) the respective national file reference;	
(c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;	(c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;	(c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;	
(d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;	(d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;	(d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;	
(e) where applicable the use of the urgent procedure referred to in Article 19(3) and the decision taken with regard to the ex-post verification;	(e) where applicable the use of the urgent procedure referred to in Article 19(3) and the decision taken with regard to the ex-post verification;	(e) where applicable the use of the urgent procedure referred to in Article 19(3) and the decision taken with regard to the ex-post verification;	

<p>(f) the data used for comparison;</p>	<p>(f) the data used for comparison;</p>	<p>(f) the data used for comparison;</p>	
<p>(g) according to national rules or the rules of the Europol decision the identifying mark of the official who carried out the search and of the official who ordered the search or supply.</p>	<p>(g) according to national rules or the rules of the Europol decision the identifying mark of the official who carried out the search and of the official who ordered the search or supply.</p>	<p>(g) according to national rules or the rules of the Europol decision the identifying mark of the official who carried out the search and of the official who ordered the search or supply.</p>	
<p>3. Such logs or documentation shall be used only for the data protection monitoring of the lawfulness of data processing as well as to ensure data security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 38. The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data</p>	<p>3. Such logs or documentation shall be used only for the data protection monitoring of the lawfulness of data processing as well as to ensure data security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 38. The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data</p>	<p>3. Such logs or documentation shall be used only for the data protection monitoring of the lawfulness of data processing as well as to ensure data security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 38. The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data</p>	<p>Identical</p> <p>Technical - the reference should be made to Art. 40 of the Dublin Regulation</p>

processing and data integrity and security, shall have access to these logs at their request for the purpose of fulfilling their duties.	processing and data integrity and security, shall have access to these logs at their request for the purpose of fulfilling their duties.	processing and data integrity and security, shall have access to these logs at their request for the purpose of fulfilling their duties.	
<i>Article 37 47</i> Liability	<i>Article 37 47</i> Liability	<i>Article 37 47</i> Liability	
1. Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with the provisions laid down in this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event giving rise to the damage.	1. Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with the provisions laid down in this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event giving rise to the damage.	1. Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with the provisions laid down in this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event giving rise to the damage.	Identical

<p>2. If failure of a Member State to comply with its obligations under this Regulation causes damage to the central database ⇒ Central System ⇐, that Member State shall be held liable for such damage, unless and insofar as the Commission ⇒ Agency or another Member State ⇐ failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.</p>	<p>2. If failure of a Member State to comply with its obligations under this Regulation causes damage to the central database ⇒ Central System ⇐, that Member State shall be held liable for such damage, unless and insofar as the Commission ⇒ Agency or another Member State ⇐ failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.</p>	<p>2. If failure of a Member State to comply with its obligations under this Regulation causes damage to the central database ⇒ Central System ⇐, that Member State shall be held liable for such damage, unless and insofar as the Commission ⇒ Agency or another Member State ⇐ failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.</p>	<p>Identical</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.</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.</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.</p>	<p>Identical</p>

CHAPTER VIII	CHAPTER VIII	CHAPTER VIII	
AMENDMENTS TO THE REGULATION (EU) No 1077/2011	AMENDMENTS TO THE REGULATION (EU) No 1077/2011	AMENDMENTS TO THE REGULATION (EU) No 1077/2011	
<i>Article 38</i> Provisions amending Regulation (EU) No 1077/2011	<i>Article 38</i> Provisions amending Regulation (EU) No 1077/2011	<i>Article 38</i> Provisions amending Regulation (EU) No 1077/2011	Identical
1. Article 5 is replaced by the following:	1. Article 5 is replaced by the following:	1. Article 5 is replaced by the following:	
<i>“Article 5</i> <i>Tasks relating to EURODAC</i>	<i>“Article 5</i> <i>Tasks relating to EURODAC</i>	<i>“Article 5</i> <i>Tasks relating to EURODAC</i>	
In relation to EURODAC, the Agency shall perform :	In relation to EURODAC, the Agency shall perform :	In relation to EURODAC, the Agency shall perform :	
(a) the tasks conferred on the Agency by Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../....}].	(a) the tasks conferred on the Agency by Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../....}].	(a) the tasks conferred on the Agency by Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../....}].	

(b) tasks relating to training on the technical use of EURODAC.”	(b) tasks relating to training on the technical use of EURODAC.”	(b) tasks relating to training on the technical use of EURODAC.”	
2. Article 12(1) is amended as follows:	2. Article 12(1) is amended as follows:	2. Article 12(1) is amended as follows:	
(a) points (t), (u) and (v) are replaced by the following:	(a) points (t), (u) and (v) are replaced by the following:	(a) points (t), (u) and (v) are replaced by the following:	
“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JH A respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and	“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JH A respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and	“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JH A respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and	

<p>Article 17(3) of Decision 2008/633/JH A; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No .../... <i>[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...} establishing the criteria and mechanisms for</i></p>	<p>Article 17(3) of Decision 2008/633/JH A; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No .../... <i>[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...} establishing the criteria and mechanisms for</i></p>	<p>Article 17(3) of Decision 2008/633/JH A; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No .../... <i>[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...} establishing the criteria and mechanisms for</i></p>	
---	---	---	--

<p>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 to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes;</p>	<p>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 to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes;</p>	<p>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 to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes;</p>	
<p>(u) to adopt the annual report</p>	<p>(u) to adopt the annual report</p>	<p>(u) to adopt the annual report</p>	

<p>on the activities of the Central System of EURODAC pursuant to Article 40(1) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];</p>	<p>on the activities of the Central System of EURODAC pursuant to Article 40(1) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];</p>	<p>on the activities of the Central System of EURODAC pursuant to Article 40(1) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];</p>	
<p>(v) to make comments on the European Data</p>	<p>(v) to make comments on the European Data</p>	<p>(v) to make comments on the European Data</p>	

<p>Protection Supervisor's reports on the audits pursuant to Article 45 of Regulation (EC) 1987/2006 , Article 42(2) of Regulation (EC) No 767/2008 and Article 31 (2) of Regulation (EU) No/..... <i>[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation</i></p>	<p>Protection Supervisor's reports on the audits pursuant to Article 45 of Regulation (EC) 1987/2006 , Article 42(2) of Regulation (EC) No 767/2008 and Article 31 (2) of Regulation (EU) No/..... <i>[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation</i></p>	<p>Protection Supervisor's reports on the audits pursuant to Article 45 of Regulation (EC) 1987/2006 , Article 42(2) of Regulation (EC) No 767/2008 and Article 31 (2) of Regulation (EU) No/..... <i>[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation</i></p>	<p>Technical - reference should be made to Art. 45(2) of Regulation (EC) 1987/2006</p>
--	--	--	--

<p>(EU) No .../....] and ensure appropriate follow-up of the audit;”</p>	<p>(EU) No .../....] and ensure appropriate follow-up of the audit;”</p>	<p>(EU) No .../....] and ensure appropriate follow-up of the audit;”</p>	
<p>(b) point (x) is replaced by the following:</p>	<p>(b) point (x) is replaced by the following:</p>	<p>(b) point (x) is replaced by the following:</p>	
<p>“(x) to compile statistics on the work of the Central System of EURODAC pursuant to Article 8(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints</p>	<p>“(x) to compile statistics on the work of the Central System of EURODAC pursuant to Article 8(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints</p>	<p>“(x) to compile statistics on the work of the Central System of EURODAC pursuant to Article 8(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints</p>	

for the effective application of Regulation (EU) No {.../....}]”	for the effective application of Regulation (EU) No {.../....}]”	for the effective application of Regulation (EU) No {.../....}]”	
(c) point (z) is replaced by the following:	(c) point (z) is replaced by the following:	(c) point (z) is replaced by the following:	
“(z) to ensure annual publication of the list of authorities designated pursuant to Article 27(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints	“(z) to ensure annual publication of the list of authorities designated pursuant to Article 27(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints	“(z) to ensure annual publication of the list of authorities designated pursuant to Article 27(2) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints	

for the effective application of Regulation (EU) No .../....]”	for the effective application of Regulation (EU) No .../....]”	for the effective application of Regulation (EU) No .../....]”	
3. In Article 15 paragraph (4) is replaced by the following:	3. In Article 15 paragraph (4) is replaced by the following:	3. In Article 15 paragraph (4) is replaced by the following:	
<p>“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, is</p>	<p>“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, is</p>	<p>“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, is</p>	

<p>on the agenda or when a question concerning EURODAC, in relation with the application of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../....]is on the agenda.”</p>	<p>on the agenda or when a question concerning EURODAC, in relation with the application of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../....]is on the agenda.”</p>	<p>on the agenda or when a question concerning EURODAC, in relation with the application of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../....]is on the agenda.”</p>	
<p>4. Article 17 is amended as follows:</p>	<p>4. Article 17 is amended as follows:</p>	<p>4. Article 17 is amended as follows:</p>	
<p>(a) in paragraph 5 point (g) is replaced by the following:</p>	<p>(a) in paragraph 5 point (g) is replaced by the following:</p>	<p>(a) in paragraph 5 point (g) is replaced by the following:</p>	
<p>“(g) without prejudice to Article 17 of the Staff Regulations,</p>	<p>“(g) without prejudice to Article 17 of the Staff Regulations,</p>	<p>“(g) without prejudice to Article 17 of the Staff Regulations,</p>	

<p>establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA and Article 26(9) of Regulation (EC) No 767/2008 respectively and Article 4(6) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the</p>	<p>establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA and Article 26(9) of Regulation (EC) No 767/2008 respectively and Article 4(6) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the</p>	<p>establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA and Article 26(9) of Regulation (EC) No 767/2008 respectively and Article 4(6) of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the</p>	
---	---	---	--

<p><i>comparison of fingerprints for the effective application of Regulation (EU) No .../...];”</i></p>	<p><i>comparison of fingerprints for the effective application of Regulation (EU) No .../...];”</i></p>	<p><i>comparison of fingerprints for the effective application of Regulation (EU) No .../...];”</i></p>	
<p>(b) in paragraph 6 point (i) is replaced by the following:</p>	<p>(b) in paragraph 6 point (i) is replaced by the following:</p>	<p>(b) in paragraph 6 point (i) is replaced by the following:</p>	
<p>“(i) reports on the technical functioning of each large-scale IT system referred to in point (t) of Article 12(1) and the annual report on the activities of the Central System of EURODAC referred to in point (u) of Article 12(1),</p>	<p>“(i) reports on the technical functioning of each large-scale IT system referred to in point (t) of Article 12(1) and the annual report on the activities of the Central System of EURODAC referred to in point (u) of Article 12(1),</p>	<p>“(i) reports on the technical functioning of each large-scale IT system referred to in point (t) of Article 12(1) and the annual report on the activities of the Central System of EURODAC referred to in point (u) of Article 12(1),</p>	

on the basis of the results of monitoring and evaluation."	on the basis of the results of monitoring and evaluation."	on the basis of the results of monitoring and evaluation."	
5. In Article 19 paragraph 3 is replaced by the following:	5. In Article 19 paragraph 3 is replaced by the following:	5. In Article 19 paragraph 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 to the EURODAC Advisory Groups."	"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 to the EURODAC Advisory Groups."	"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 to the EURODAC Advisory Groups."	
CHAPTER VII IX	CHAPTER VII IX	CHAPTER VII IX	
FINAL PROVISIONS	FINAL PROVISIONS	FINAL PROVISIONS	
<i>Article 39 21</i> Costs	<i>Article 39 21</i> Costs	<i>Article 39 21</i> Costs	Identical
1. The costs incurred in	1. The costs incurred in	1. The costs incurred in	

<p>connection with the establishment and operation of the Central Unit ⇒ Central System and the Communication Infrastructure ⇐ shall be borne by the general budget of the European Union.</p>	<p>connection with the establishment and operation of the Central Unit ⇒ Central System and the Communication Infrastructure ⇐ shall be borne by the general budget of the European Union.</p>	<p>connection with the establishment and operation of the Central Unit ⇒ Central System and the Communication Infrastructure ⇐ shall be borne by the general budget of the European Union.</p>	
<p>2. The costs incurred by national ⇐ access points ⇐ units and the costs for connection to the central database ⇒ Central System ⇐ shall be borne by each Member State.</p>	<p>2. The costs incurred by national ⇐ access points ⇐ units and the costs for connection to the central database ⇒ Central System ⇐ shall be borne by each Member State.</p>	<p>2. The costs incurred by national ⇐ access points ⇐ units and the costs for connection to the central database ⇒ Central System ⇐ shall be borne by each Member State.</p>	
<p>3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of</p>	<p>3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of</p>	<p>3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of</p>	

the criminal offences defined in this Regulation.	the criminal offences defined in this Regulation.	the criminal offences defined in this Regulation.	
3. The costs of transmission of data from the Member State of origin and of the findings of the comparison to that State shall be borne by the State in question.	3. The costs of transmission of data from the Member State of origin and of the findings of the comparison to that State shall be borne by the State in question.	3. The costs of transmission of data from the Member State of origin and of the findings of the comparison to that State shall be borne by the State in question.	
<i>Article 40 24</i> Annual report, mMonitoring and evaluation	<i>Article 40 24</i> Annual report, mMonitoring and evaluation	<i>Article 40 24</i> Annual report, mMonitoring and evaluation	
1. The Commission ⇒ Agency ⇐ shall submit to the European Parliament and the Council an annual report on the activities of the Central Unit ⇒ System ⇐. The annual report shall include information on the management and performance of Eurodac EURODAC against pre-defined quantitative indicators for the objectives referred to	1. The Commission ⇒ Agency ⇐ shall submit to the European Parliament and the Council an annual report on the activities of the Central Unit ⇒ System ⇐. The annual report shall include information on the management and performance of Eurodac EURODAC against pre-defined quantitative indicators for the objectives referred to	1. The Commission ⇒ Agency ⇐ shall submit to the European Parliament and the Council an annual report on the activities of the Central Unit ⇒ System ⇐. The annual report shall include information on the management and performance of Eurodac EURODAC against pre-defined quantitative indicators for the objectives referred to	Identical

in paragraph 2.	in paragraph 2.	in paragraph 2.	
<p>2. The Commission ⇒ Agency ⇐ shall ensure that ⊗ procedures ⊗ systems are in place to monitor the functioning of the Central Unit ⇒ System ⇐ against objectives ⊗ relating to ⊗ in terms of outputs, cost-effectiveness and quality of service.</p>	<p>2. The Commission ⇒ Agency ⇐ shall ensure that ⊗ procedures ⊗ systems are in place to monitor the functioning of the Central Unit ⇒ System ⇐ against objectives ⊗ relating to ⊗ in terms of outputs, cost-effectiveness and quality of service.</p>	<p>2. The Commission ⇒ Agency ⇐ shall ensure that ⊗ procedures ⊗ systems are in place to monitor the functioning of the Central Unit ⇒ System ⇐ against objectives ⊗ relating to ⊗ in terms of outputs, cost-effectiveness and quality of service.</p>	Identical
<p>3. The Commission shall regularly evaluate the operation of the Central Unit in order to establish whether its objectives have been attained cost-effectively and with a view to providing guidelines for improving the efficiency of future operations.</p>	<p>3. The Commission shall regularly evaluate the operation of the Central Unit in order to establish whether its objectives have been attained cost-effectively and with a view to providing guidelines for improving the efficiency of future operations.</p>	<p>3. The Commission shall regularly evaluate the operation of the Central Unit in order to establish whether its objectives have been attained cost-effectively and with a view to providing guidelines for improving the efficiency of future operations.</p>	
<p>4. One year after Eurodae starts operations, the Commission shall produce an evaluation report on the Central Unit, focusing on the level of demand</p>	<p>4. One year after Eurodae starts operations, the Commission shall produce an evaluation report on the Central Unit, focusing on the level of demand</p>	<p>4. One year after Eurodae starts operations, the Commission shall produce an evaluation report on the Central Unit, focusing on the level of demand</p>	

<p>compared with expectation and on operational and management issues in the light of experience, with a view to identifying possible short-term improvements to operational practice.</p>	<p>compared with expectation and on operational and management issues in the light of experience, with a view to identifying possible short-term improvements to operational practice.</p>	<p>compared with expectation and on operational and management issues in the light of experience, with a view to identifying possible short-term improvements to operational practice.</p>	
<p>3. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in the Central System.</p>	<p>3. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in the Central System.</p>	<p>3. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in the Central System.</p>	Identical
<p>4. Every two years, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.</p>	<p>4. Every <i>year</i>, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.</p>	<p>4. Every two years, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.</p>	EP and Council to further consider, at technical level, the EP amendment

5. Three years after ~~Eurodac~~ starts operations ⇒ the start of application of this Regulation as provided for in Article 46(2) ⇐ and every ~~six~~ ⇒ four ⇐ years thereafter, the Commission shall produce an overall evaluation of ~~Eurodac~~ EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations ⇒ , as well as make any necessary recommendations ⇐ . ⇒ The Commission shall transmit the evaluation to the European Parliament and the Council. ⇐

5. Three years after the start of application of this Regulation as provided for in Article 46(2) 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 the indirect discrimination of persons covered by this Regulation,*** and assessing the continuing validity of the underlying rationale, and any implications for future operations, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

5. Three years after ~~Eurodac~~ starts operations ⇒ the start of application of this Regulation as provided for in Article 46(2) ⇐ and every ~~six~~ ⇒ four ⇐ years thereafter, the Commission shall produce an overall evaluation of ~~Eurodac~~ EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations ⇒ , as well as make any necessary recommendations ⇐ . ⇒ The Commission shall transmit the evaluation to the European Parliament and the Council. ⇐

By way of compromise the Cion suggest the following wording (in bold / underline):

Three years after the start of application of this Regulation as provided for in Article 46(2) and every four years thereafter, the Commission shall produce an overall evaluation of EURODAC, examining ***the*** results achieved against objectives, ***the impact on fundamental rights, including whether law enforcement access has led to the indirect discrimination of persons covered by this Regulation,*** and assessing the continuing validity of the underlying rationale, and any implications for future operation, as well as make any necessary recommendations. ***The Commission shall also evaluate whether the [three/five] year period laid down in Article 18(2) shall be modified.*** The Commission shall transmit the evaluation to the European Parliament and the Council.

The Pres recommends acceptance

			of the Cion compromise
6. Member States shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraph 4 and 5.	6. Member States shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraph 4 and 5.	6. Member States shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraph 4 and 5.	Identical
7. The Agency shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.	7. The Agency shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.	7. ☞ [...] ☛	Deletion agreed
8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison,	8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, <i>grounds given for reasonable suspicion,</i>	8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison,	As a result of the third informal trilogue the following compromise has been provisionally agreed upon for this provision by EP and the Pres (<i>a deadline for submission of data by Member States is suggested, in order to make the timely preparation of the annual report by the Cion, under this provision, feasible</i>): 8. In accordance with national legislation, each Member State and Europol shall prepare annual reports on the effectiveness of the comparison

<p>the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.</p>	<p>number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission. <i>On the basis of these annual reports and in addition to the overall evaluation provided for in paragraph 5, the Commission shall compile an annual report on law enforcement access to EURODAC and shall transmit the evaluation to the European Parliament, the Council and the European Data Protection Supervisor.</i></p>	<p>the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.</p>	<p>of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, grounds given for reasonable suspicion, the reasonable grounds given not to conduct comparison with other Member States under Council Decision 2008/615/JHA, in accordance with Article 20(1), number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission before 30 June of the subsequent year. On the basis of these annual reports and in addition to the overall evaluation provided for in paragraph 5, the Commission shall compile an annual report on law enforcement access to</p>
---	---	---	---

			<p>EURODAC and shall transmit the evaluation to the European Parliament, the Council and the European Data Protection Supervisor.</p> <p>The Pres recommends acceptance of the compromise, without prejudice to further discussions with the EP on the inclusions of the wording "In accordance with national legislation" at the beginning of the paragraph.</p>
<p>9. The Agency, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.</p>	<p>9. The Agency, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.</p>	<p>9. The Agency, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.</p>	<p>Identical</p>

<p align="center"><i>Article 41 25</i> Penalties</p>	<p align="center"><i>Article 41 25</i> Penalties</p>	<p align="center"><i>Article 41 25</i> Penalties</p>	
<p>Member States shall <input checked="" type="checkbox"/> take the necessary measures to <input checked="" type="checkbox"/> ensure that <input checked="" type="checkbox"/> any <input checked="" type="checkbox"/> <u>processing use</u> of data recorded <input checked="" type="checkbox"/> entered <input checked="" type="checkbox"/> in the central database <input checked="" type="checkbox"/> Central System <input checked="" type="checkbox"/> contrary to the purpose of EurodacEURODAC as laid down in Article 1(1) shall be subject to appropriate penalties <input checked="" type="checkbox"/> is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive <input checked="" type="checkbox"/>.</p>	<p>Member States shall <input checked="" type="checkbox"/> take the necessary measures to <input checked="" type="checkbox"/> ensure that <input checked="" type="checkbox"/> any <input checked="" type="checkbox"/> <u>processing use</u> of data recorded <input checked="" type="checkbox"/> entered <input checked="" type="checkbox"/> in the central database <input checked="" type="checkbox"/> Central System <input checked="" type="checkbox"/> contrary to the purpose of EurodacEURODAC as laid down in Article 1(1) shall be subject to appropriate penalties <input checked="" type="checkbox"/> is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive <input checked="" type="checkbox"/>.</p>	<p>Member States shall <input checked="" type="checkbox"/> take the necessary measures to <input checked="" type="checkbox"/> ensure that <input checked="" type="checkbox"/> any <input checked="" type="checkbox"/> <u>processing use</u> of data recorded <input checked="" type="checkbox"/> entered <input checked="" type="checkbox"/> in the central database <input checked="" type="checkbox"/> Central System <input checked="" type="checkbox"/> contrary to the purpose of EurodacEURODAC as laid down in Article 1 <input checked="" type="checkbox"/> [...] <input checked="" type="checkbox"/> shall be subject to appropriate penalties <input checked="" type="checkbox"/> is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive <input checked="" type="checkbox"/>.</p>	<p>Council amendment accepted by the EP</p>
<p align="center"><i>Article 42 26</i> Territorial scope</p>	<p align="center"><i>Article 42 26</i> Territorial scope</p>	<p align="center"><i>Article 42 26</i> Territorial scope</p>	
<p>The provisions of this Regulation shall not be applicable to any territory</p>	<p>The provisions of this Regulation shall not be applicable to any territory</p>	<p>The provisions of this Regulation shall not be applicable to any territory</p>	<p align="center">Identical</p>

to which the Dublin Convention ☒ Regulation ☒ does not apply.	to which the Dublin Convention ☒ Regulation ☒ does not apply.	to which the Dublin Convention ☒ Regulation ☒ does not apply.	
Article 43 Notification of designated authorities and verifying authorities	Article 43 Notification of designated authorities and verifying authorities	Article 43 Notification of designated authorities and verifying authorities	
1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its designated authorities and shall notify without delay any amendment thereto.	1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its designated authorities and of the operating units referred to in Article 5(3) and shall notify without delay any amendment thereto.	1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its designated authorities and shall notify without delay any amendment thereto.	EP compromise accepted (the word "operating" should be replaced by "operational").
	1a. Each Member State shall constantly update the information it has provided to the Commission. The Commission shall make that information available to the other Member States, Europol		By way of compromise, Cion suggests deletion of this EP amendment (see also new para. 4a)

	<i>and the public via a constantly updated electronic publication.</i>		
2. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its verifying authority and shall notify without delay any amendment thereto.	2. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its verifying authority and shall notify without delay any amendment thereto.	2. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its verifying authority and shall notify without delay any amendment thereto.	Identical
	<i>2a. Europol shall constantly update the information it has provided to the Commission. The Commission shall make this information available to the other Member States and the public via a constantly updated electronic publication.</i>		By way of compromise, Cion suggests deletion of this EP amendment (see also new para. 4a)
3. By [three months after the date of entry into force of this Regulation] at the latest Europol shall notify the Commission of its verifying authority and	3. By [three months after the date of entry into force of this Regulation] at the latest Europol shall notify the Commission of its verifying authority and	3. By [three months after the date of entry into force of this Regulation] at the latest Europol shall notify the Commission of its verifying authority and	Identical

the National Access Point which it has designated and shall notify without delay any amendment thereto.	the National Access Point which it has designated and shall notify without delay any amendment thereto.	the National Access Point which it has designated and shall notify without delay any amendment thereto.	
4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the <i>Official Journal of the European Union</i> on an annual basis.	4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the <i>Official Journal of the European Union</i> on an annual basis.	4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the <i>Official Journal of the European Union</i> on an annual basis.	Identical
			<p>The Cion suggests the following new paragraph to replace paragraphs 1a and 2a:</p> <p><u>4a. The Commission shall publish information referred to in paragraphs 1, 2 and 3 via an electronic publication that is available online and updated without delay.</u></p> <p>The Pres recommends acceptance</p>
Article 44 Transitional provision	Article 44 Transitional provision	Article 44 Transitional provision	
Data blocked in the Central System in accordance with Article	Data blocked in the Central System in accordance with Article	Data blocked in the Central System in accordance with Article	This Article is linked with the scope of Art. 18 (under negotiations)

12 of Council Regulation (EC) No 2725/2000/EC shall be unblocked and marked in accordance with Article 18(1) of this Regulation on the date provided for in Article 46 of this Regulation.	12 of Council Regulation (EC) No 2725/2000/EC shall be unblocked and marked in accordance with Article 18(1) of this Regulation on the date provided for in Article 46 of this Regulation.	12 of Council Regulation (EC) No 2725/2000/EC shall be unblocked and marked in accordance with Article 18(1) of this Regulation on the date provided for in Article 46 of this Regulation.	Technical - reference should be made to Art. 46(2) of the Regulation
Article 45 Repeal	Article 45 Repeal	Article 45 Repeal	Identical
Council Regulation (EC) No 2725/2000 of 11 December 2000 and Council Regulation (EC) No 407/2002 are repealed with effect from the date referred to in Article 46(2).	Council Regulation (EC) No 2725/2000 of 11 December 2000 and Council Regulation (EC) No 407/2002 are repealed with effect from the date referred to in Article 46(2).	Council Regulation (EC) No 2725/2000 of 11 December 2000 and Council Regulation (EC) No 407/2002 are repealed with effect from the date referred to in Article 46(2).	
References to the repealed Regulations shall be read in accordance with the correlation table in Annex III.	References to the repealed Regulations shall be read in accordance with the correlation table in Annex III.	References to the repealed Regulations shall be read in accordance with the correlation table in Annex III.	

<p style="text-align: center;"><i>Article 46 27</i> Entry into force and applicability</p>	<p style="text-align: center;"><i>Article 46 27</i> Entry into force and applicability</p>	<p style="text-align: center;"><i>Article 46 27</i> Entry into force and applicability</p>	<p style="text-align: center;">Identical</p>
<p>1. This Regulation shall enter into force on the ⊗ twentieth ⊗ day ⊗ following that ⊗ of its publication in the Official Journal of the European Communities ⊗ Union ⊗.</p>	<p>1. This Regulation shall enter into force on the ⊗ twentieth ⊗ day ⊗ following that ⊗ of its publication in the Official Journal of the European Communities ⊗ Union ⊗.</p>	<p>1. This Regulation shall enter into force on the ⊗ twentieth ⊗ day ⊗ following that ⊗ of its publication in the Official Journal of the European Communities ⊗ Union ⊗.</p>	
<p>2. This Regulation shall apply ⇒ two years from the date of the entry into force of this Regulation. ↵ □, — and Eurodac shall start operations, from the date which the Commission shall publish in the Official Journal of the European Communities, when the following conditions met:</p>	<p>2. This Regulation shall apply ⇒ two years from the date of the entry into force of this Regulation. ↵ □, — and Eurodac shall start operations, from the date which the Commission shall publish in the Official Journal of the European Communities, when the following conditions met:</p>	<p>2. This Regulation shall apply ⇒ two years from the date of the entry into force of this Regulation. ↵ □, — and Eurodac shall start operations, from the date which the Commission shall publish in the Official Journal of the European Communities, when the following conditions met:</p>	
<p>(a) each Member State has notified the Commission that it has made the necessary technical</p>	<p>(a) each Member State has notified the Commission that it has made the necessary technical</p>	<p>(a) each Member State has notified the Commission that it has made the necessary technical</p>	

<p>arrangements to transmit data to the Central Unit in accordance with the implementing rules adopted under Article 4(7) and to comply with the implementing rules adopted under Article 12(5); and</p>	<p>arrangements to transmit data to the Central Unit in accordance with the implementing rules adopted under Article 4(7) and to comply with the implementing rules adopted under Article 12(5); and</p>	<p>arrangements to transmit data to the Central Unit in accordance with the implementing rules adopted under Article 4(7) and to comply with the implementing rules adopted under Article 12(5); and</p>	
<p>(b) the Commission has made the necessary technical arrangements for the Central Unit to begin operations in accordance with the implementing rules adopted under Article 4(7) and Article 12(5).</p>	<p>(b) the Commission has made the necessary technical arrangements for the Central Unit to begin operations in accordance with the implementing rules adopted under Article 4(7) and Article 12(5).</p>	<p>(b) the Commission has made the necessary technical arrangements for the Central Unit to begin operations in accordance with the implementing rules adopted under Article 4(7) and Article 12(5).</p>	
<p>3. Member States shall notify the Commission and the Agency as soon as they have made the technical arrangements to transmit data to the Central System, and in any event no later than two years from the date</p>	<p>3. Member States shall notify the Commission and the Agency as soon as they have made the technical arrangements to transmit data to the Central System, and in any event no later than two years from the date</p>	<p>3. Member States shall notify the Commission and the Agency as soon as they have made the technical arrangements to transmit data to the Central System, and in any event no later than two years from the date</p>	

of the entry into force of this Regulation.	of the entry into force of this Regulation.	of the entry into force of this Regulation.	
4. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.	4. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.	4. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.	
Done at Brussels,	Done at Brussels,	Done at Brussels,	
<i>For the European Parliament For the Council</i>	<i>For the European Parliament For the Council</i>	<i>For the European Parliament For the Council</i>	
<i>The President The President</i>	<i>The President The President</i>	<i>The President The President</i>	