

Amended proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
1.	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	
2.	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), Article 74, Article 77(2)(a) (b) (d) and (e) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), Article 74, Article 77(2)(a) (b) (d) and (e) thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), Article 74, Article 77(2)(a) (b) (d) and (e) thereof,	
3.	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
4.	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	
5.	After consulting the European Data Protection Supervisor,	After consulting the European Data Protection Supervisor,	After consulting the European Data Protection Supervisor,	
6.	Having regard to the opinion of the European Economic and Social Committee, ¹	Having regard to the opinion of the European Economic and Social Committee, ²	Having regard to the opinion of the European Economic and Social Committee, ³	
7.	Having regard to the opinion of the Committee of the Regions, ⁴	Having regard to the opinion of the Committee of the Regions, ⁵	Having regard to the opinion of the Committee of the Regions, ⁶	
8.	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	
9.	Whereas:	Whereas:	Whereas:	

¹ OJ C , , p. .

² OJ C , , p. .

³ OJ C , , p. .

⁴

⁵

⁶

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
10.	<p>(1) In its Communication of 6 April 2016 entitled <i>Stronger and Smarter Information Systems for Borders and Security</i>⁷, the Commission underlined the need to improve the Union's data management architecture for border management and security. The Communication initiated a process towards achieving the interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to these systems that impede the work of national authorities and to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.</p>	<p>(1) In its Communication of 6 April 2016 entitled <i>Stronger and Smarter Information Systems for Borders and Security</i>⁸, the Commission underlined the need to improve the Union's data management architecture for border management and security. The Communication initiated a process towards achieving the interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to these systems that impede the work of national authorities and to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.</p>	<p>(1) In its Communication of 6 April 2016 entitled <i>Stronger and Smarter Information Systems for Borders and Security</i>⁹, the Commission underlined the need to improve the Union's data management architecture for border management and security. The Communication initiated a process towards achieving the interoperability between EU information systems for security, border and migration management, with the aim to address the structural shortcomings related to these systems that impede the work of national authorities and to ensure that border guards, customs authorities, police officers and judicial authorities have the necessary information at their disposal.</p>	

⁷ COM(2016)205, 6.4.2016.

⁸ COM(2016)205, 6.4.2016.

⁹ COM(2016)205, 6.4.2016.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
11.	(2) In its Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area of 6 June 2016 ¹⁰ , the Council identified various legal, technical and operational challenges in the interoperability of EU information systems and called for the pursuit of solutions.	(2) In its Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area of 6 June 2016 ¹¹ , the Council identified various legal, technical and operational challenges in the interoperability of EU information systems and called for the pursuit of solutions.	(2) In its Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area of 6 June 2016 ¹² , the Council identified various legal, technical and operational challenges in the interoperability of EU information systems and called for the pursuit of solutions.	
12.	(3) In its Resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ¹³ , the European Parliament called for proposals to improve and develop existing EU	(3) In its Resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ¹⁴ , the European Parliament called for proposals to improve and develop existing EU	(3) In its Resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ¹⁵ , the European Parliament called for proposals to improve and develop existing EU	

¹⁰ Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

¹¹ Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

¹² Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area — 9368/1/16 REV 1.

¹³ European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ([2016/2773\(RSP\)](#)).

¹⁴ European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ([2016/2773\(RSP\)](#)).

¹⁵ European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 ([2016/2773\(RSP\)](#)).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	information systems, address information gaps and move towards their interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by the necessary data protection safeguards.	information systems, address information gaps and move towards their interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by the necessary data protection safeguards.	information systems, address information gaps and move towards their interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by the necessary data protection safeguards.	
13.	(4) The European Council of 15 December 2016 ¹⁶ called for continued delivery on the interoperability of EU information systems and databases.	(4) The European Council of 15 December 2016 ¹⁷ called for continued delivery on the interoperability of EU information systems and databases.	(4) The European Council of 15 December 2016 ¹⁸ called for continued delivery on the interoperability of EU information systems and databases.	
14.	(5) In its final report of 11 May 2017 ¹⁹ , the high-level expert group on information systems and interoperability concluded that it is necessary and technically feasible to work towards practical solutions for interoperability and that they	(5) In its final report of 11 May 2017 ²⁰ , the high-level expert group on information systems and interoperability concluded that it is necessary and technically feasible to work towards practical solutions for interoperability and that they	(5) In its final report of 11 May 2017 ²¹ , the high-level expert group on information systems and interoperability concluded that it is necessary and technically feasible to work towards practical solutions for interoperability and that they	

¹⁶ <http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/>.

¹⁷ <http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/>.

¹⁸ <http://www.consilium.europa.eu/en/press/press-releases/2016/12/15/euco-conclusions-final/>.

¹⁹ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&cid=32600&no=1>.

²⁰ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&cid=32600&no=1>.

²¹ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&cid=32600&no=1>.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	can, in principle, both deliver operational gains and be established in compliance with data protection requirements.	can, in principle, both deliver operational gains and be established in compliance with data protection requirements.	can, in principle, both deliver operational gains and be established in compliance with data protection requirements.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
15.	(6) In its Communication of 16 May 2017 entitled <i>Seventh progress report towards an effective and genuine Security Union</i> ²² , the Commission set out, in line with its Communication of 6 April 2016 and confirmed by the findings and recommendations of the high-level expert group on information systems and interoperability, a new approach to the management of data for borders, security and migration where all EU information systems for security, border and migration management are interoperable in full respect of fundamental rights.	(6) In its Communication of 16 May 2017 entitled <i>Seventh progress report towards an effective and genuine Security Union</i> ²³ , the Commission set out, in line with its Communication of 6 April 2016 and confirmed by the findings and recommendations of the high-level expert group on information systems and interoperability, a new approach to the management of data for borders, security and migration where all EU information systems for security, border and migration management are interoperable in full respect of fundamental rights.	(6) In its Communication of 16 May 2017 entitled <i>Seventh progress report towards an effective and genuine Security Union</i> ²⁴ , the Commission set out, in line with its Communication of 6 April 2016 and confirmed by the findings and recommendations of the high-level expert group on information systems and interoperability, a new approach to the management of data for borders, security and migration where all EU information systems for security, border and migration management are interoperable in full respect of fundamental rights.	

²² COM(2017) 261 final, 16.5.2017.

²³ COM(2017) 261 final, 16.5.2017.

²⁴ COM(2017) 261 final, 16.5.2017.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
16.	(7) In its Conclusions of 9 June 2017 ²⁵ on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to pursue the solutions for interoperability as proposed by the high-level expert group.	(7) In its Conclusions of 9 June 2017 ²⁶ on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to pursue the solutions for interoperability as proposed by the high-level expert group.	(7) In its Conclusions of 9 June 2017 ²⁷ on the way forward to improve information exchange and ensure the interoperability of EU information systems, the Council invited the Commission to pursue the solutions for interoperability as proposed by the high-level expert group.	
17.	(8) The European Council of 23 June 2017 ²⁸ underlined the need to improve the interoperability between databases and invited the Commission to prepare, as soon as possible, draft legislation enacting the proposals made by the high-level expert group on information systems and interoperability.	(8) The European Council of 23 June 2017 ²⁹ underlined the need to improve the interoperability between databases and invited the Commission to prepare, as soon as possible, draft legislation enacting the proposals made by the high-level expert group on information systems and interoperability.	(8) The European Council of 23 June 2017 ³⁰ underlined the need to improve the interoperability between databases and invited the Commission to prepare, as soon as possible, draft legislation enacting the proposals made by the high-level expert group on information systems and interoperability.	

²⁵ <http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf>.

²⁶ <http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf>.

²⁷ <http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf>.

²⁸ [European Council conclusions](#), 22-23 June 2017.

²⁹ [European Council conclusions](#), 22-23 June 2017.

³⁰ [European Council conclusions](#), 22-23 June 2017.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
18.		<i>(8a) In his Opinion 4/2018 of 16 April 2018³¹, the European Data Protection Supervisor emphasised that the decision to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a ‘point of no return’.</i>		
19.		<i>(8b) In its Opinion of 11 April 2018³², the Article 29 Data Protection Working Party reiterated that the process towards interoperability of systems raises fundamental questions regarding the purpose, necessity, proportionality of the data processing as well as concerns regarding the principles of purpose limitation,</i>		

³¹ http://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf

³² http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51517

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>data minimization, data retention and clear identification of a data controller.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
20.	<p>(9) With a view to improve the management of the external borders, to contribute to preventing and combating irregular migration and to contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States, interoperability between EU information systems, namely [the Entry/Exit System (EES)], the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and the [European Criminal Records Information System for third-country nationals (ECRIS-TCN)] should be established in order for these EU information systems and their data to supplement each other. To achieve this, a</p>	<p>(9) With a view <i>In order</i> to improve the management of the external borders, <i>to facilitating regular border crossings</i>, to contribute to preventing and combating irregular migration and to contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States, <i>to improve the implementation of the common visa policy and to assist in examining applications for international protection, and to assist in the prevention, detection and investigation of terrorist offences or other serious criminal offences, in order to maintain public trust in the Union migration and asylum system, Union security measures and Union capabilities to manage the external border,</i> interoperability between EU</p>	<p>(9) With a view to improve the <i>effectiveness and efficiency of checks at</i> management of the external borders, to contribute to preventing and combating irregular <i>illegal immigration</i> and to contribute to a high level of security within the area of freedom, security and justice of the Union, including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States, <i>to improve the implementation of the common visa policy, to assist in examining applications lodged in a Member State,</i> interoperability between EU information systems, namely {the Entry/Exit System (EES)}, the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and the [European Criminal Records</p>	

	<p style="text-align: center;">Amended Commission proposal</p> <p style="text-align: center;">(ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate</p> <p style="text-align: center;">(ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.</p>	<p><i>Union</i> information systems, namely the {Entry/Exit System (<i>the</i> EES)}, the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and the [European Criminal Records Information System for third-country nationals (ECRIS-TCN)] should be established in order for these EU <i>Union</i> information systems and their data to supplement each other <i>so far as that is possible while respecting the fundamental rights of the individual, in particular the right to protection of personal data.</i> To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.</p>	<p>Information System for third-country nationals (ECRIS-TCN)] should be established in order for these EU information systems and their data to supplement each other. To achieve this, a European search portal (ESP), a shared biometric matching service (shared BMS), a common identity repository (CIR) and a multiple-identity detector (MID) should be established as interoperability components.</p>	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>21.</p>	<p>(10) The interoperability between the EU information systems should allow said systems to supplement each other in order to facilitate the correct identification of persons, contribute to fighting identity fraud, improve and harmonise data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of existing and future EU information systems, strengthen and simplify the data security and data protection safeguards that govern the respective EU information systems, streamline the law enforcement access to the EES, the VIS, the [ETIAS] and Eurodac, and support the purposes of the EES, the VIS, the [ETIAS], Eurodac, the SIS and the [ECRIS-TCN system].</p>	<p>(10) The interoperability between the EU Union information systems should allow said systems to supplement each other in order to facilitate the correct identification of persons, <i>for the purpose of applications of international protection or in the context of the prevention, detection and investigation of serious criminal offences - including terrorist offences, to contribute to fighting identity fraud, improve and harmonise data quality requirements of the respective EU Union information systems, facilitate the technical and operational implementation by Member States of existing and future EU to contribute to ensuring the effective use of Union information systems, Europol data and Interpol databases by facilitating access to them by the authorities in accordance with their access rights and the objectives and purposes as laid down in the</i></p>	<p>(10) The interoperability between the EU information systems should allow said systems to supplement each other in order to facilitate the correct identification of persons, <i>including unknown persons who are not able to identify themselves or unidentified remains</i>, contribute to fighting identity fraud, improve and harmonise data quality requirements of the respective EU information systems, facilitate the technical and operational implementation by Member States of existing and future EU information systems, strengthen and simplify the data security and data protection safeguards that govern the respective EU information systems, streamline the law enforcement access <i>for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences</i> to the EES, the</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p><i>legal instruments governing the respective systems, to strengthen and simplify and harmonise the data security and data protection safeguards that govern the respective Union information systems, in particular by ensuring that all Union data protection rules are applicable to all the EU information systems, and to streamline the law enforcement and simplify designated authorities access to the EES, the VIS, the [ETIAS] and Eurodac, and support the purposes of the EES, the VIS, the [ETIAS], Eurodac, the SIS and the [ECRIS-TCN system].</i></p>	<p>VIS, the [ETIAS] and Eurodac, and support the purposes of the EES, the VIS, the [ETIAS], Eurodac, the SIS and the [ECRIS-TCN system].</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
22.	(11) The interoperability components should cover the EES, the VIS, the [ETIAS], Eurodac, the SIS, and the [ECRIS-TCN system]. They should also cover the Europol data to the extent of enabling it to be queried simultaneously with these EU information systems.	(11) The interoperability components should cover the EES, the VIS, the [ETIAS], Eurodac, the SIS, and the [ECRIS-TCN system]. They should also cover the Europol data only to the extent of enabling it that data to be queried simultaneously with these EU Union information systems.	(11) The interoperability components should cover the EES, the VIS, the [ETIAS], Eurodac, the SIS, and the [ECRIS-TCN system]. They should also cover the Europol data to the extent of enabling it to be queried simultaneously with these EU information systems.	
23.	(12) The interoperability components should concern persons in respect of whom personal data may be processed in the EU information systems and by Europol, namely third-country nationals whose personal data is processed in the EU information systems and by Europol, and to EU citizens whose personal data is processed in the SIS and by Europol.	(12) The interoperability components should concern persons in respect of whom personal data may be processed in the EU information systems and by Europol, namely third-country nationals whose personal data is processed in the EU information systems and by Europol, and to EU citizens whose personal data is processed in the SIS and by Europol.	(12) The interoperability components should concern persons in respect of whom personal data may be processed in the EU information systems and by Europol, namely third-country nationals persons whose personal data is are processed in the EU information systems and by Europol, and to including EU citizens whose personal data is are processed in the SIS and by Europol.	
24.		<i>(12a) Children and vulnerable persons merit specific protection with regard to their personal data, as they may be less aware</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. The interoperability components should be designed so that particular attention is paid to the protection of children and that their rights and integrity are fully respected.</i>		

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>25.</p>	<p>(13) The European search portal (ESP) should be established to facilitate technically the ability of Member State authorities and EU bodies to have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases needed to perform their tasks, in accordance with their access rights, and to support the objectives of the EES, the VIS, the [ETIAS], Eurodac, the SIS, the [ECRIS-TCN system] and the Europol data. Enabling the simultaneous querying of all relevant EU information systems in parallel, as well as of the Europol data and the Interpol databases, the ESP should act as a single window or ‘message broker’ to search various central systems and retrieve the necessary information seamlessly and in full respect of the access control and data protection requirements of the underlying</p>	<p>(13) The European search portal (ESP) should be established to facilitate technically the ability of <i>the authorised</i> Member State authorities and EU bodies <i>Union agencies</i> to have fast, seamless, efficient, systematic and controlled access to the <i>relevant Union</i> EU information systems, the Europol data and the Interpol databases <i>insofar as this is</i> needed to perform their tasks, in accordance with their access rights, and to support the objectives of the EES, the VIS, the [ETIAS], Eurodac, the SIS, the [ECRIS-TCN system] and the Europol data. Enabling the simultaneous querying of all relevant EU <i>Union</i> information systems in parallel, as well as of the Europol data and the Interpol databases, the ESP should act as a single window or ‘message broker’ to search various central systems and retrieve the necessary information seamlessly</p>	<p>(13) The European search portal (ESP) should be established to facilitate technically the ability of Member State authorities and EU bodies <i>agencies</i> to have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases needed to perform their tasks, in accordance with their access rights, and to support the objectives of the EES, the VIS, the [ETIAS], Eurodac, the SIS, the [ECRIS-TCN system] and the Europol data. Enabling the simultaneous querying of all relevant EU information systems in parallel, as well as of the Europol data and the Interpol databases, the ESP should act as a single window or ‘message broker’ to search various central systems and retrieve the necessary information seamlessly and in full respect of the access control and data protection</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	systems.	and in full respect of the access control and data protection requirements of the underlying systems.	requirements of the underlying systems.	
26.			<i>(13a) When querying the Interpol databases, the design of the ESP should ensure that the data used by the user of the ESP to launch a query is not shared with the owners of Interpol data. The result of the query should not be shared in an automated manner with the owner of the Interpol data and a positive result should only be shared following the assessment of the competent authorities including the Interpol National Central Bureau of the Member State querying the Interpol databases.</i>	
27.	(14) The International Criminal Police Organisation (Interpol) database of Stolen and Lost Travel Documents (SLTD) enables authorised law enforcement entities in Member	(14) The International Criminal Police Organisation (Interpol) database of Stolen and Lost Travel Documents (SLTD) enables authorised law enforcement entities in Member	(14) The International Criminal Police Organisation (Interpol) database of Stolen and Lost Travel Documents (SLTD) enables authorised law enforcement entities responsible	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<p>States, including immigration and border control officers, to establish the validity of a travel document. The [ETIAS] queries the SLTD and Interpol's Travel Documents Associated with Notices (TDAWN) database in the context of assessing whether a person applying for a travel authorisation is likely for instance to migrate irregularly or could pose a threat to security. The centralised European search portal (ESP) should enable the query against the SLTD and TDAWN databases using an individual's identity data. Where personal data are transferred from the Union to Interpol through the ESP, the provisions on international transfers in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council³³, or the national</p>	<p>States, including immigration and border control officers, to establish the validity of a travel document. The [ETIAS] queries the SLTD and Interpol's Travel Documents Associated with Notices (TDAWN) database in the context of assessing whether a person applying for a travel authorisation is likely for instance to migrate irregularly or could pose a threat to security. The centralised European search portal (ESP) should enable the query against the SLTD and TDAWN databases using an individual's identity data. Where personal data are transferred from the Union to Interpol through the ESP, the provisions on international transfers in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council³⁷, or the national</p>	<p><i>for preventing, detecting or investigating terrorist offences or other serious criminal offences</i> in Member States, including immigration and border control officers, to establish the validity of a travel document. The [ETIAS] queries the SLTD and Interpol's Travel Documents Associated with Notices (TDAWN) database in the context of assessing whether a person applying for a travel authorisation is likely for instance to migrate irregularly or could pose a threat to security. The centralised European search portal (ESP) should enable the query against the SLTD and TDAWN databases using an individual's identity data <i>or travel document data</i>. Where personal data are transferred from the Union to Interpol through the</p>	

³³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council ³⁴ should apply. This should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA ³⁵ and Council Decision 2007/533/JHA ³⁶ .	provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council³⁸ should apply. This should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA³⁹ and Council Decision 2007/533/JHA⁴⁰.	ESP, the provisions on international transfers in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council ⁴¹ , or the national provisions transposing Chapter V of Directive (EU) 2016/680 of the European Parliament and of the Council ⁴² should apply. This	

³⁷ ~~Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).~~

³⁴ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

³⁵ Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).

³⁶ Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

³⁸ ~~Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).~~

³⁹ ~~Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).~~

⁴⁰ ~~Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).~~

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA ⁴³ and Council Decision 2007/533/JHA ⁴⁴ .	
28.	(15) The European search portal (ESP) should be developed and configured in such a way that it does not allow the use of fields of data for the query that are not related to persons or travel documents or that are not present in an EU information system, in the Europol data or in the Interpol database.	(15) The European search portal (ESP) should be developed and configured in such a way that it does not allow the use of fields of data for the query that are not related to persons or travel documents or that are not present in an EU information system, in the Europol data or in the Interpol database.	(15) The European search portal (ESP) should be developed and configured in such a way that it does not allow the use of fields of data for the query that are not related to persons or travel documents or that are not present in an EU information system, in the Europol data or in the Interpol database.	

⁴¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

⁴² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

⁴³ Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).

⁴⁴ Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>29.</p>	<p>(16) To ensure fast and systematic use of all EU information systems, the European search portal (ESP) should be used to query the common identity repository, the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system]. However, the national connection to the different EU information systems should remain in order to provide a technical fall back. The ESP should also be used by Union bodies to query the Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query the Central SIS, the Europol data and the Interpol systems, complementing the existing dedicated interfaces.</p>	<p>(16) To ensure fast and systematic <i>seamless</i> use of all relevant Union EU information systems, the European search portal (ESP) should be used to query the common identity repository, the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system]. <i>A central Union backup ESP should be established in order to provide all the functionalities of the principal ESP and a similar level of performance as it in the event of its failure.</i> However, the national connection to the different relevant Union EU information systems should remain in order to provide a technical fall back. The ESP should also be used by Union bodies <i>agencies</i> to query the Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query the Central SIS, the Europol data and the Interpol</p>	<p>(16) To ensure fast and systematic use of all EU information systems, the European search portal (ESP) should be used to query the common identity repository, the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system]. However, the national connection to the different EU information systems should remain in order to provide a technical fall back. The ESP should also be used by Union bodies <i>agencies</i> to query the Central SIS in accordance with their access rights and in order to perform their tasks. The ESP should be an additional means to query the Central SIS, the Europol data and the Interpol systems, complementing the existing dedicated interfaces.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		systems, complementing the existing dedicated interfaces.		
30.	(17) Biometric data, such as fingerprints and facial images, are unique and therefore much more reliable than alphanumeric data for identifying a person. The shared biometric matching service (shared BMS) should be a technical tool to reinforce and facilitate the work of the relevant EU information systems and the other interoperability components. The main purpose of the shared BMS should be to facilitate the identification of an individual who may be registered in different databases, by matching their biometric data across different systems and by relying on one unique technological component instead of five different ones in each of the underlying systems. The shared BMS should contribute to security, as well as financial, maintenance and operational	(17) Biometric data, <i>that in the content of this regulation entails such as fingerprints and facial images only and therefore excludes hand palm prints</i> , are unique and therefore much more reliable than alphanumeric data for identifying a person. <i>However, biometric data constitute sensitive personal data. This Regulation should therefore lay down the basis of and the safeguards for processing of such data for the purpose of uniquely identifying the persons concerned.</i> The shared biometric matching service (Shared BMS) should be a technical tool to reinforce and facilitate the work of the relevant EU <i>Union</i> information systems, <i>the effective use of Europol data</i> and the other interoperability components. <i>The SBMS should replace the Automated</i>	(17) Biometric data, such as fingerprints <i>dactyloscopic data</i> and facial images, are unique and therefore much more reliable than alphanumeric data for identifying a person. The shared biometric matching service (shared BMS) should be a technical tool to reinforce and facilitate the work of the relevant EU information systems and the other interoperability components. The main purpose of the shared BMS should be to facilitate the identification of an individual who may be registered in different databases, by matching their biometric data across different systems and by relying on one unique technological component instead of five different ones in each of the underlying systems. The shared BMS should contribute to security, as well as financial,	

	<p align="center">Amended Commission proposal (ST 10178/18)</p>	<p align="center">EP amendments</p>	<p align="center">Council negotiation mandate (ST 11312/18)</p>	<p align="center">Compromise text proposals</p>
	<p>benefits by relying on one unique technological component instead of different ones in each of the underlying systems. All automated fingerprint identification systems, including those currently used for Eurodac, the VIS and the SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples. The shared BMS should regroup and store all these biometric templates in one single location, facilitating cross-system comparisons using biometric data and enabling economies of scale in developing and maintaining the EU central systems.</p>	<p><i>Fingerprint Identification Systems of respectively the EES, VIS, SIS, Eurodac and [ECRIS-TCN] and should therefore not duplicate either the storage of the biometric data nor the storage of biometric templates.</i> The main purpose of the shared BMS should be to facilitate the identification of an individual who may be registered in different databases, by matching their biometric data across different systems and by relying on one unique technological component instead of five different ones in each of the underlying systems. The shared BMS should contribute to security, as well as financial, maintenance and operational benefits by relying on one unique technological component instead of different ones in each of the underlying systems. All automated fingerprint identification systems, including those currently used for Eurodac,</p>	<p>maintenance and operational benefits by relying on one unique technological component instead of different ones in each of the underlying systems. All automated fingerprint identification systems, including those currently used for Eurodac, the VIS and the SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples. The shared BMS should regroup and store all these biometric templates in one single location, facilitating cross-system comparisons using biometric data and enabling economies of scale in developing and maintaining the EU central systems.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p>the VIS and the SIS, use biometric templates comprised of data derived from a feature extraction of actual biometric samples. The shared BMS should regroup and store all these biometric templates – <i>logically separated according to the information system from which the data originated</i> – in one single location, <i>thereby</i> facilitating cross-system comparisons using biometric data <i>templates</i> and enabling economies of scale in developing and maintaining the EU <i>Union</i> central systems.</p>		
31.		<p><i>(17a) The biometric templates stored in the shared BMS which are comprised of data derived from a feature extraction of actual biometric samples should be obtained in such a way that reverting the process is not possible. Indeed, biometric templates should be obtained from biometric data but it should</i></p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>not be possible to obtain that same biometric data from the biometric templates.</i>		
32.	(18) Biometric data constitute sensitive personal data. This regulation should lay down the basis for and the safeguards for processing of such data for the purpose of uniquely identifying the persons concerned.	(18) — Biometric data constitute sensitive personal data. This regulation should lay down the basis for and the safeguards for processing of such data for the purpose of uniquely identifying the persons concerned.	(18) Biometric data constitute sensitive personal data. This Regulation should lay down the basis for and the safeguards for processing of such data for the purpose of uniquely identifying the persons concerned.	
33.	(19) The systems established by Regulation (EU) 2017/2226 of the European Parliament and of the Council ⁴⁵ , Regulation (EC) No 767/2008 of the European Parliament and of the Council ⁴⁶ ,	(19) The systems established by Regulation (EU) 2017/2226 of the European Parliament and of the Council ⁴⁷ , Regulation (EC) No 767/2008 of the European Parliament and of the Council ⁴⁸ ,	(19) The systems established by Regulation (EU) 2017/2226 of the European Parliament and of the Council ⁴⁹ , Regulation (EC) No 767/2008 of the European Parliament and of the Council ⁵⁰ ,	

⁴⁵ Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (EES Regulation) (OJ L 327, 9.12.2017, p. 20–82).

⁴⁶ Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

⁴⁷ Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (EES Regulation) (OJ L 327, 9.12.2017, p. 20–82).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	[the ETIAS Regulation] for the management of the borders of the Union, the system established by [the Eurodac Regulation] to identify the applicants for international protection and combat irregular migration, and the system established by [the ECRIS-TCN system Regulation] require in order to be effective to rely on the accurate identification of the third-country nationals whose personal data are stored therein.	[the ETIAS Regulation] for the management of the borders of the Union, the system established by [the Eurodac Regulation] to identify the applicants for international protection and combat irregular migration, and the system established by [the ECRIS-TCN system Regulation] require in order to be effective to rely on the accurate identification of <i>those</i> the third-country nationals whose personal data are stored therein.	[the ETIAS Regulation] for the management of the borders of the Union, the system established by [the Eurodac Regulation] to identify the applicants for international protection and combat irregular <i>illegal</i> immigration, and the system established by [the ECRIS-TCN system Regulation] require in order to be effective to rely on the accurate identification of the third-country nationals <i>persons</i> whose personal data are stored therein.	
34.	(20) The common identity repository (CIR) should therefore facilitate and assist in the correct	(20) The common identity repository (CIR) should therefore facilitate and assist in the correct	(20) The common identity repository (CIR) should therefore facilitate and assist in the correct	

⁴⁸ Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

⁴⁹ Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (EES Regulation) (OJ L 327, 9.12.2017, p. 20–82).

⁵⁰ Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	identification of persons registered in the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system].	identification of persons registered in the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system].	identification of persons registered in the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system].	
35.	(21) Personal data stored in these EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory, but the same is not true for third-country nationals. The interoperability between EU information systems should contribute to the correct identification of third-country nationals. The common identity repository (CIR) should store the personal data concerning third-country nationals present in the systems that are necessary to enable the more accurate identification of those individuals, therefore including their identity, travel document and biometric data, regardless of	(21) Personal data stored in these EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory, but the same is not true for third-country nationals. The interoperability between EU information systems should contribute to the correct identification of third-country nationals. The common identity repository (CIR) should store the personal data concerning third-country nationals present in the systems that are necessary to enable the more accurate identification of those individuals, therefore including their identity, travel document and biometric data, regardless of	(21) Personal data stored in these EU information systems may relate to the same persons but under different or incomplete identities. Member States dispose of efficient ways to identify their citizens or registered permanent residents in their territory, but the same is not true for <i>other categories of persons</i> third-country nationals . The interoperability between EU information systems should contribute to the correct identification of <i>those persons</i> third-country nationals . The common identity repository (CIR) should store the personal data concerning third-country nationals <i>those persons</i> present in the systems that are necessary to enable the more accurate identification of those	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>the system in which the data was originally collected. Only the personal data strictly necessary to perform an accurate identity check should be stored in the CIR. The personal data recorded in the CIR should be kept for no longer than is strictly necessary for the purposes of the underlying systems and should be automatically deleted when the data is deleted in the underlying systems in accordance with their logical separation.</p>	<p>the system in which the data was originally collected. Only the personal data strictly necessary to perform an accurate identity check should be stored in the CIR. The personal data recorded in the CIR should be kept for no longer than is strictly necessary for the purposes of the underlying systems and should be automatically deleted when the data is deleted in the underlying systems in accordance with their logical separation.</p>	<p>individuals, therefore including their identity, travel document and biometric data, regardless of the system in which the data was originally collected. Only the personal data strictly necessary to perform an accurate identity check should be stored in the CIR. The personal data recorded in the CIR should be kept for no longer than is strictly necessary for the purposes of the underlying systems and should be automatically deleted when the data <i>are</i> is deleted in the underlying systems in accordance with their logical separation. <i>However, for the purpose of fighting identity fraud, where a red link is stored in the MID, the linked identity and travel document data should be stored in the CIR for as long as the corresponding data are stored in at least one of the EU information systems from which the linked data originates.</i></p>	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>36.</p>	<p>(22) The new processing operation consisting in the storage of such data in the common identity repository (CIR) instead of the storage in each of the separate systems is necessary to increase the accuracy of the identification that is made possible by the automated comparison and matching of such data. The fact that the identity and biometric data of third-country nationals is stored in the CIR should not hinder in any way the processing of data for the purposes of the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system Regulations, as the CIR should be a new shared component of those underlying systems.</p>	<p>(22) The new processing operation consisting in the storage of such data in the common identity repository (CIR) instead of the storage in each of the separate systems is necessary to increase the accuracy of the identification that is made possible by the automated comparison and matching of such data. The fact that the identity and biometric data of third-country nationals is stored in the CIR should not hinder in any way the processing of data for the purposes of the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system Regulations, as the CIR should be a new shared component of those underlying systems.</p>	<p>(22) The new processing operation consisting in the storage of such data in the common identity repository (CIR) instead of the storage in each of the separate systems is necessary to increase the accuracy of the identification that is made possible by the automated comparison and matching of such data. The fact that the identity, <i>travel document</i> and biometric data of third-country nationals is <i>are</i> stored in the CIR should not hinder in any way the processing of data for the purposes of the EES, the VIS, <i>[the ETIAS]</i>, Eurodac or the ECRIS-TCN system Regulations, as the CIR should be a new shared component of those underlying systems.</p>	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>37.</p>	<p>(23) In that connection, creating an individual file in the common identity repository (CIR) for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system, is necessary to achieve the purpose of correct identification of third-country nationals within the Schengen area, and to support the multiple-identity detector for the dual purpose of facilitating identity checks for <i>bona fide</i> travellers and combating identity fraud. The individual file should store in one single place and make accessible to the duly authorised end-users all the possible identities linked to a person.</p>	<p>(23) In that connection, creating an individual file in the common identity repository (CIR) for each person that is recorded in the EES, the VIS, the ETIAS, Eurodac or the ECRIS-TCN system, is necessary to achieve the purpose of correct identification of third-country nationals within the Schengen area, and to support the multiple-identity detector for the dual purpose of facilitating identity checks for <i>bona fide</i> travellers and combating identity fraud. The individual file should store in one single place and make accessible to the duly authorised end-users all the possible identities linked to a person.</p>	<p>(23) In that connection, creating an individual file in the common identity repository (CIR) for each person that is recorded in the EES, the VIS, <i>[the ETIAS]</i>, Eurodac or <i>[the ECRIS-TCN system]</i>, is necessary to achieve the purpose of correct identification of <i>each person</i> third-country nationals within the Schengen area, and to support the multiple-identity detector for the dual purpose of facilitating identity checks for <i>bona fide</i> travellers and combating identity fraud. The individual file should store in one single place and make accessible to the duly authorised end-users all the possible identities linked to a person.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
38.	(24) The common identity repository (CIR) should thus support the functioning of the multiple-identity detector and to facilitate and streamline access by law enforcement authorities to the EU information systems that are not established exclusively for purposes of prevention, investigation, detection or prosecution of serious crime.	(24) The common identity repository (CIR) should thus support the functioning of the multiple-identity detector and to facilitate and streamline access by law enforcement authorities to the EU information systems that are not established exclusively for purposes of prevention, investigation, detection or prosecution of serious crime.	(24) The common identity repository (CIR) should thus support the functioning of the multiple-identity detector and to facilitate and streamline access by law enforcement authorities <i>responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences</i> to the EU information systems that are not established exclusively for purposes of prevention, investigation or detection or prosecution of serious crime.	
39.	(25) The common identity repository (CIR) should provide for a shared container for identity and biometric data of third-country nationals registered in the EES, the VIS, [the ETIAS], Eurodac and the [ECRIS-TCN system], serving as the shared component between these systems for storage of this data, and to allow its querying.	(25) The common identity repository (CIR) should provide for a shared container for identity and biometric data of third-country nationals registered in the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system], serving as the shared component between these systems for storage of this data, and to allow its querying. <i>A central Union backup CIR</i>	(25) The common identity repository (CIR) should provide for a shared container for identity, <i>travel document</i> and biometric data of third-country nationals <i>persons</i> registered in the EES, the VIS, [the ETIAS], Eurodac and the [ECRIS-TCN system]. <i>It should be part of the technical architecture of these systems and serve</i> serving as the shared component between these	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>should be established in order to provide all the functionalities of the principal CIR and a similar level of performance as it in the event of its failure.</i>	systems <i>them</i> for storage of this <i>the identity, travel document and biometric</i> data, and to allow its <i>their</i> querying.	
40.	(26) All records in the common identity repository (CIR) should be logically separated by automatically tagging each record with the underlying system owning that record. The access control of the CIR should use these tags to allow the record to be accessible or not.	(26) All records in the common identity repository (CIR) should be logically separated by automatically tagging each record with the underlying system owning that record. The access control of the CIR should use these tags to allow the record to be accessible or not.	(26) All records in the common identity repository (CIR) should be logically separated by automatically tagging each record with the underlying system owning that record. The access control of the CIR should use these tags to allow the record to be accessible or not.	
41.	(27) In order to ensure the correct identification of a person, Member State authorities competent for preventing and combating irregular migration and competent authorities within the meaning of Article 3(7) of Directive 2016/680 should be allowed to query the common identity repository (CIR) with the biometric data of that person taken during an identity check.	(27) In order to ensure <i>assist in</i> ensure the correct identification of a person, where a Member State authorities competent for preventing and combating irregular migration and <i>police authority has been unable to identify that person on the basis of a query of the CIR using a travel document or the identity data provided by that person, or where there are doubts as to the</i>	(27) In order to ensure the correct identification of a person, <i>police authorities empowered by national law</i> Member State authorities competent for preventing and combating irregular migration and competent authorities within the meaning of Article 3(7) of Directive 2016/680 should be allowed to query the common identity repository (CIR) with the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>authenticity of the travel document or the identity of its holder, or where the person is unable or refuses to cooperate, a Member State</i> competent authorities within the meaning of Article 3(7) of Directive 2016/680, <i>following rules and procedures provided for in national law</i> , should be allowed to query the common identity repository (CIR) with the biometric data of that person taken during an identity check, <i>provided always that the person concerned is physically present during such a check.</i>	biometric data of that person taken during an identity check.	
42.	(28) Where the biometric data of the person cannot be used or if the query with that data fails, the query should be carried out with identity data of that person in combination with travel document data. Where the query indicates that data on that person are stored in the common identity repository (CIR), Member State authorities should have access to	(28) —Where the biometric data of the person cannot be used or if the query with that data fails, the query should be carried out with identity data of that person in combination with travel document data. Where the query indicates that data on that person are stored in the common identity repository (CIR), Member State authorities should have access to	(28) Where the biometric data of the person cannot be used or if the query with that data fails, the query should be carried out with identity data of that person in combination with travel document data. Where the query indicates that data on that person are stored in the common identity repository (CIR), Member State authorities should have access to	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	consult the identity data of that person stored in the CIR, without providing any indication as to which EU information system the data belongs to.	consult the identity data of that person stored in the CIR, without providing any indication as to which EU information system the data belongs to.	consult the identity data <i>and travel document data</i> of that person stored in the CIR, without providing any indication as to which EU information system the data belongs to.	
43.	(29) Member States should adopt national legislative measures designating the authorities competent to perform identity checks with the use of the common identity repository (CIR) and laying down the procedures, conditions and criteria of such checks in line with the principle of proportionality. In particular, the power to collect biometric data during an identity check of a person present before the member of those authorities should be provided for by national legislative measures.	(29) Member States should adopt national legislative measures designating the authorities competent to perform identity checks with the use of the common identity repository (CIR) and laying down the procedures, conditions and criteria of such checks in line with the principle of proportionality. In particular, the power to collect biometric data during an identity check of a person present before the member of those authorities should be provided for by national legislative measures.	(29) Member States should adopt national legislative measures designating the authorities competent to perform identity checks with the use of the common identity repository (CIR) and laying down the procedures, conditions and criteria of such checks in line with the principle of proportionality. In particular, the power to collect biometric data during an identity check of a person present before the member of those authorities should be provided for by national <i>law</i> legislative measures.	
44.	(30) This Regulation should also introduces a new possibility for streamlined access to data beyond identity data present in	(30) This Regulation should also introduces a new possibility for streamlined access to data beyond identity data present in	(30) This Regulation should also introduces a new possibility for streamlined access to data beyond identity data <i>or travel</i>	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>the EES, the VIS, [the ETIAS] or Eurodac by Member State designated law enforcement authorities and Europol. Data, including data other than identity data contained in those systems, may be necessary for the prevention, detection, investigation and prosecution of terrorist offences or serious criminal offences in a specific case.</p>	<p>the EES, the VIS, [the ETIAS] or Eurodac by Member State designated law enforcement authorities and Europol. Data, including data other than identity data contained in those systems, may be necessary for the prevention, detection, investigation and prosecution of terrorist offences or serious criminal offences in a specific case <i>where there are reasonable grounds to consider that consultation will substantially contribute to the prevention, detection or investigation of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under the category of third-country nationals whose data are stored in the EES, VIS, ETIAS and Eurodac. Such streamlined access should be provided after a prior search in</i></p>	<p><i>document data</i> present in the EES, the VIS, [the ETIAS] or Eurodac by Member State designated law enforcement authorities <i>responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences</i> and Europol. Data, including data other than identity data <i>or travel document data</i> contained in those systems, may be necessary for the prevention, detection, investigation and prosecution of terrorist offences or serious criminal offences in a specific case.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>the national databases has been carried out and a query of the automated fingerprint identification system of the other Member States under Council Decision 2008/615/JHA⁵¹ has been launched.</i>		
45.	(31) Full access to the necessary data contained in the EU information systems necessary for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences, beyond the relevant identity data covered under common identity repository (CIR) obtained using biometric data of that person taken during an identity check, should continue to be governed by the provisions in the respective legal instruments. The designated law enforcement authorities and Europol do not	(31) Full access to the necessary data contained in the Union EU-information systems necessary for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences, beyond the relevant identity data covered under common identity repository (CIR) obtained using biometric data of that person taken during an identity check, should continue to be governed by the provisions in the respective legal instruments. The designated law enforcement authorities and Europol do not	(31) Full access to the necessary data contained in the EU information systems necessary for the purposes of preventing, detecting and or investigating terrorist offences or other serious criminal offences, beyond the relevant identity data or travel document data covered under common identity repository (CIR) obtained using biometric data of that person taken during an identity check, should continue to be governed by the provisions in the respective legal instruments. The designated law enforcement authorities	

⁵¹ Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<p>know in advance which of the EU information systems contains data of the persons they need to inquire upon. This results in delays and inefficiencies in the conduct of their tasks. The end-user authorised by the designated authority should therefore be allowed to see in which of the EU information systems the data corresponding to the query introduced are recorded. The concerned system would thus be flagged following the automated verification of the presence of a hit in the system (a so-called hit-flag functionality).</p>	<p>know in advance which of the Union EU information systems contains data of the persons they need to inquire upon. This results in delays and inefficiencies in the conduct of their tasks. The end-user authorised by the designated authority should therefore be allowed to see in which of the EU Union information systems the data corresponding to the query introduced are recorded. The concerned system would thus be flagged following the automated verification of the presence of a hit in the system (a so-called hit-flag functionality) <i>after necessary checks in national databases and after a query of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA has been launched.</i></p>	<p><i>responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences</i> and Europol do not know in advance which of the EU information systems contains data of the persons they need to inquire upon. This results in delays and inefficiencies in the conduct of their tasks. The end-user authorised by the designated authority should therefore be allowed to see in which of the EU information systems the data corresponding to the query introduced are recorded. The concerned system would thus be flagged following the automated verification of the presence of a match hit in the system (a so-called hit match-flag functionality).</p>	
46.			<p><i>(31a) The reply will not be interpreted and used as a ground or reason to draw conclusions</i></p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>on or undertake measures towards a person, but may be used only for the purpose of submitting an access request to the underlying EU information systems, subject to the conditions and procedures laid down in the respective legislative instruments governing such access. Any such act will be subject to measures set out in Chapter VII and measures in Regulation (EU) 2016/679, Directive 2016/680 or Regulation (EC) No 45/2001.</i>	
47.	(32) The logs of the queries of the common identity repository should indicate the purpose of the query. Where such a query was performed using the two-step data consultation approach, the logs should include a reference to the national file of the investigation or case, therefore indicating that such query was launched for the purposes of preventing, detecting and investigating terrorist offences or	(32) The logs of the queries of the common identity repository should indicate the purpose of the query. Where such a query was performed using the two-step data consultation approach, the logs should include a reference to the national file of the investigation or case, therefore indicating that such query was launched for the purposes of preventing, detecting and investigating terrorist offences or	(32) The logs of the queries of the common identity repository should indicate the purpose of the query. Where such a query was performed using the two-step data consultation approach, the logs should include a reference to the national file of the investigation or case, therefore indicating that such query was launched for the purposes of preventing, detecting and <i>or</i> investigating terrorist offences or	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	other serious criminal offences.	other serious criminal offences.	other serious criminal offences.	
48.	(33) The query of the common identity repository (CIR) by Member State designated authorities and Europol in order to obtain a hit-flag type of response indicating the data is recorded in the EES, the VIS, [the ETIAS] or Eurodac requires automated processing of personal data. A hit-flag would not reveal personal data of the concerned individual other than an indication that some of his or her data are stored in one of the systems. No adverse decision for the concerned individual should be made by the authorised end-user solely on the basis of the simple occurrence of a hit-flag. Access by the end-user of a hit-flag would therefore realise a very limited interference with the right to protection of personal data of the concerned individual, while it would be necessary to allow the designated authority	(33) The query of the common identity repository (CIR) by Member State designated authorities and Europol in order to obtain a hit-flag type of response indicating the data is recorded in the EES, the VIS, [the ETIAS] or Eurodac requires automated processing of personal data. A hit-flag would not reveal only personal data of the concerned individual other than an indication that some of his or her data are stored in one of the systems, provided the authority making the search has access to that system . No adverse decision for the concerned individual should be made by the authorised end-user solely on the basis of the simple occurrence of a hit-flag, and the hit-flag should be used by the relevant authorities only for the purpose of deciding which database to query . Access by the end-user of a hit-flag	(33) The query of the common identity repository (CIR) by Member State designated authorities and Europol in order to obtain a hit match -flag type of response indicating the data is are recorded in the EES, the VIS, [the ETIAS] or Eurodac requires automated processing of personal data. A hit match -flag would not reveal personal data of the concerned individual other than an indication that some of his or her data are stored in one of the systems. No adverse decision for the concerned individual should be made by the authorised end-user solely on the basis of the simple occurrence of a hit match -flag. Access by the end-user to of a hit match -flag would therefore realise a very limited interference with the right to protection of personal data of the concerned individual, while it would be necessary to allow the designated	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>and Europol to address its request for access for personal data more effectively directly to the system that was flagged as containing it.</p>	<p>would therefore realise a very limited interference with the right to protection of personal data of the concerned individual, while it would be necessary to allow the designated authority and Europol to address its request for access for personal data more effectively directly to the system that was flagged as containing it.</p>	<p>authority and Europol to address its request for access <i>to for</i> personal data more effectively directly to the system that was flagged as containing it.</p>	
<p>49.</p>	<p>(34) The two-step data consultation approach is particularly valuable in cases where the suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is unknown. In those cases the common identity repository (CIR) should enable identifying the information system that knows the person in one single search. By creating the obligation to use this new law enforcement access approach in these cases, access to the personal data stored in the EES, the VIS, [the ETIAS] and Eurodac should take place without the</p>	<p>(34) The two-step data consultation approach is particularly valuable in cases where the suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is unknown. In those cases the common identity repository (CIR) the relevant designated authority to identify identifying the information system that knows the person in one single search. By creating the obligation to use this new law enforcement access approach in these cases, access to the personal data stored in the</p>	<p>(34) The two-step data consultation approach is particularly valuable in cases where the suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is unknown. In those cases the common identity repository (CIR) should enable identifying the information system that knows the person in one single search. By creating the obligation to use this new law enforcement access approach for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences in</p>	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA. The principle of prior search effectively limits the possibility of Member State' authorities to consult systems for justified law enforcement purposes and could thereby result in missed opportunities to uncover necessary information. The requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA should only cease to apply once the alternative safeguard of the two-step approach to law enforcement access through the CIR has become operational.</p>	<p>EES, the VIS, [the ETIAS] and Eurodac should take place without the requirements of a prior search, following the necessary checks in national databases and the launch of a prior search in once a query of the automated fingerprint identification system of other Member States under Decision 2008/615/JHA has been launched for the justified purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences should only cease to apply once the alternative safeguard of the two-step approach to law enforcement access through the CIR has become operational.</p>	<p>these cases, access to the personal data stored in the EES the VIS, [the ETIAS] and Eurodac should take place without the requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA. The principle of prior search effectively limits the possibility of Member States' authorities to consult centralised systems for the justified law enforcement purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences and could thereby result in missed opportunities to uncover necessary information. The requirements of a prior search in national databases and the launch of a prior search in the automated fingerprint identification system of other Member States under Decision 2008/615/JHA should</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			only cease to apply once the alternative safeguard of the two-step approach to law enforcement access <i>for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences</i> through the CIR has become operational.	
50.	(35) The multiple-identity detector (MID) should be established to support the functioning of the common identity repository and to support the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system]. In order to be effective in fulfilling their respective objectives, all of these EU information systems require the accurate identification of the persons whose personal data are stored therein.	(35) The multiple-identity detector (MID) should be established to support the functioning of the common identity repository and to support the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system]. In order to be effective in fulfilling their respective objectives, all of these EU information systems require the accurate identification of the persons whose personal data are stored therein.	(35) The multiple-identity detector (MID) should be established to support the functioning of the common identity repository and to support the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system]. In order to be effective in fulfilling their respective objectives, all of these EU information systems require the accurate identification of the persons whose personal data are stored therein.	
51.	(36) The possibility to achieve the objectives of the EU information systems is	(36) <i>To better realise</i> The possibility to achieve the objectives of the EU information	(36) The possibility to achieve the objectives of the EU information systems is	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>undermined by the current inability for the authorities using these systems to conduct sufficiently reliable verifications of the identities of the third-country nationals whose data are stored in different systems. That inability is determined by the fact that the set of identity data stored in a given individual system may be fraudulent, incorrect, or incomplete, and that there is currently no possibility to detect such fraudulent, incorrect or incomplete identity data by way of comparison with data stored in another system. To remedy this situation it is necessary to have a technical instrument at Union level allowing accurate identification of third-country nationals for these purposes.</p>	<p>systems is undermined by the current inability for, the authorities using these <i>those</i> systems <i>should be able</i> to conduct sufficiently reliable verifications of the identities of the third-country nationals whose data are stored in different systems. That inability is determined by the fact that The set of identity data stored in a given individual system may be <i>incorrect, incomplete or</i> fraudulent, incorrect, or incomplete, and that <i>and</i> there is currently no <i>way of detecting incorrect, incomplete or</i> possibility to detect such fraudulent, incorrect or incomplete identity data by way of comparison with data stored in another system. To remedy this situation it is necessary to have a technical instrument at Union level allowing accurate identification of third-country nationals for these purposes.</p>	<p>undermined by the current inability for the authorities using these systems to conduct sufficiently reliable verifications of the identities of the third-country nationals <i>persons</i> whose data are stored in different systems. That inability is determined by the fact that the set of identity data <i>or travel document data</i> stored in a given individual system may be fraudulent, incorrect, or incomplete, and that there is currently no possibility to detect such fraudulent, incorrect or incomplete identity data <i>or travel document data</i> by way of comparison with data stored in another system. To remedy this situation it is necessary to have a technical instrument at Union level allowing accurate identification of third-country nationals <i>persons</i> for these purposes.</p>	

	<p style="text-align: center;">Amended Commission proposal</p> <p style="text-align: center;">(ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate</p> <p style="text-align: center;">(ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>52.</p>	<p>(37) The multiple-identity detector (MID) should create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for <i>bona fide</i> travellers and combating identity fraud. The MID should only contain the links between individuals present in more than one EU information system, strictly limited to the data necessary to verify that a person is recorded lawfully or unlawfully under different biographical identities in different systems, or to clarify that two persons having similar biographical data may not be the same person. Data processing through the European search portal (ESP) and the shared biometric matching service (shared BMS) in order to link individual files across individual systems should be kept to an absolute minimum and therefore</p>	<p>(37) The multiple-identity detector (MID) should create and store links between data in the different EU Union information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud. The <i>creation of those links constitutes automated decision-making as referred to in Regulation (EU) 2016/679 and Directive (EU) 2016/680 and therefore requires transparency towards the individuals affected and the implementation of necessary safeguards in accordance with Union data protection rules. The MID</i> should only contain the links <i>only</i> between individuals present in more than one EU Union information system, strictly limited to the data necessary to verify that a person is recorded lawfully or unlawfully under different biographical identities in</p>	<p>(37) The multiple-identity detector (MID) should create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud. The MID should only contain the links between individuals present in more than one EU information system, strictly limited to the data necessary to verify that a person is recorded in a justified lawfully or unlawfully unjustified manner under different biographical identities in different systems, or to clarify that two persons having similar biographical data may not be the same person. Data processing through the European search portal (ESP) and the shared biometric matching service (shared BMS) in order to link individual files across individual systems should be kept to an absolute minimum and</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	is limited to a multiple-identity detection at the time new data is added to one of the information systems included in the common identity repository and in the SIS. The MID should include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities.	different systems, or to clarify that two persons having similar biographical data may not be the same person. Data processing through the European search portal (ESP) and the shared biometric matching service (shared BMS) in order to link individual files across individual systems <i>and the Europol database</i> should be kept to an absolute minimum and therefore is limited to a multiple-identity detection at the time new data is added to one of the <i>Union</i> information systems included in the common identity repository and in the SIS. The MID should include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities.	therefore is limited to a multiple-identity detection at the time new data <i>are</i> is added to one of the information systems included in the common identity repository and in the SIS. The MID should include safeguards against potential discrimination or unfavourable decisions for persons with multiple lawful identities.	
53.	(38) This Regulation provides for new data processing operations aimed at identifying the persons concerned correctly.	(38) This Regulation provides for new data processing operations aimed at identifying the persons concerned correctly.	(38) This Regulation provides for new data processing operations aimed at identifying the persons concerned correctly.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	This constitutes an interference with their fundamental rights as protected by Articles 7 and 8 of the Charter of Fundamental Rights. Since the effective implementation of the EU information systems is dependent upon correct identification of the individuals concerned, such interference is justified by the same objectives for which each of those systems have been established, the effective management of the Union's borders, the internal security of the Union, the effective implementation of the Union's asylum and visa policies and the fight against irregular migration.	This constitutes an interference with their fundamental rights as protected by Articles 7 and 8 of the Charter of Fundamental Rights. Since the effective implementation of the EU information systems is dependent upon correct identification of the individuals concerned, such interference is justified by the same objectives for which each of those systems have been established, the effective management of the Union's borders, the internal security of the Union, the effective implementation of the Union's asylum and visa policies and the fight against irregular migration.	This constitutes an interference with their fundamental rights as protected by Articles 7 and 8 of the Charter of Fundamental Rights. Since the effective implementation of the EU information systems is dependent upon correct identification of the individuals concerned, such interference is justified by the same objectives for which each of those systems have been established, the effective management of the Union's borders, the internal security of the Union, the effective implementation of the Union's asylum and visa policies and the fight against irregular illegal immigration .	
54.	(39) The European search portal (ESP) and shared biometric matching service (shared BMS) should compare data in common identity repository (CIR) and SIS on persons when new records are created by a national authority or	(39) The European search portal (ESP) and shared biometric matching service (shared BMS) should compare data in common identity repository (CIR) and SIS on persons when new records are created by a national authority or	(39) The European search portal (ESP) and shared biometric matching service (shared BMS) should compare data in common identity repository (CIR) and SIS on persons when new records are created or uploaded by a national	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<p>an EU body. Such comparison should be automated. The CIR and the SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and the SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and the SIS should be able to identify identical or similar data on the third-country national stored across several systems. Where such is the case, a link indicating that it is the same person should be established. The CIR and the SIS should be configured in such a way that small transliteration or spelling mistakes are detected in such a way as not to create any unjustified hindrance to the concerned third-country national.</p>	<p>an EU body. Such comparison should be automated. The CIR and the SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and the SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and the SIS should be able to identify identical or similar data on the third-country national stored across several systems. Where such is the case, a link indicating that it is the same person should be established. The CIR and the SIS should be configured in such a way that small transliteration or spelling mistakes are detected in such a way as not to create any unjustified hindrance to the concerned third-country national.</p>	<p>authority or an EU <i>agency body</i>. Such comparison should be automated. The CIR and the SIS should use the shared BMS to detect possible links on the basis of biometric data. The CIR and the SIS should use the ESP to detect possible links on the basis of alphanumeric data. The CIR and the SIS should be able to identify identical or similar data on the third-country national <i>person</i> stored across several systems. Where such is the case, a link indicating that it is the same person should be established. The CIR and the SIS should be configured in such a way that small transliteration or spelling mistakes are detected in such a way as not to create any unjustified hindrance to the concerned third-country national <i>person</i>.</p>	
55.	(40) The national authority or EU body that recorded the data in the respective EU information	(40) The national authority or EU body that recorded the data in the respective EU information	(40) The national authority or EU <i>agency body</i> that recorded the data in the respective EU	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	system should confirm or change these links. This authority should have access to the data stored in the common identity repository (CIR) or the SIS and in the multiple-identity detector (MID) for the purpose of the manual identity verification.	system should confirm or change these links. This authority should have access to the data stored in the common identity repository (CIR) or the SIS and in the multiple-identity detector (MID) for the purpose of the manual identity verification.	information system should confirm or change these links. This authority should have access to the data stored in the common identity repository (CIR) or the SIS and in the multiple-identity detector (MID) for the purpose of the manual identity verification.	
56.	(41) Access to the multiple-identity detector (MID) by Member State authorities and EU bodies having access to at least one EU information system included in the common identity repository (CIR) or to the SIS should be limited to so called red links where the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person, or where the linked data has similar identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to	(41) Access to the multiple-identity detector (MID) by Member State authorities and EU Union bodies having access to at least one EU Union information system included in the common identity repository (CIR) or to the SIS should be limited to so called red links where the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully in an unjustified manner to the same person, or where the linked data has similar identity data and the authority responsible for the verification of different identities	(41) Access to the multiple-identity detector (MID) by Member State authorities and EU bodies agencies having access to at least one EU information system included in the common identity repository (CIR) or to the SIS should be limited to so called red links where the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person in an unjustified manner , or where the linked data has similar different identity data, at least one of the EU information systems does not	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	the same person. Where the linked identity data is not similar, a yellow link should be established and a manual verification should take place in order to confirm the link or change its colour accordingly.	concluded it refers unlawfully in an unjustified manner to the same person. Where the linked identity data is not similar, a yellow link should be established and a manual verification should take place in order to confirm the link or change its colour accordingly.	have biometric data on the person and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person in an unjustified manner, or where the linked data have same or similar identity data, the same travel document data, but different biometric data and the authority responsible for the verification of different identities concluded it refers to different persons in an unjustified manner. Where the linked identity data are is not similar, a yellow link should be established and a manual verification should take place in order to confirm the link or change its colour accordingly.	
57.	(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a hit resulting in a link with data already stored in another EU	(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a hit resulting in a link with data already stored in another EU	(42) The manual verification of multiple identities should be ensured by the authority creating or updating the data that triggered a hit match resulting in a link with data already stored in	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	information system. The authority responsible for the verification of multiple identities should assess whether there are multiple lawful or unlawful identities. Such assessment should be performed where possible in the presence of the third-country national and where necessary by requesting additional clarifications or information. Such assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law.	information system. The authority responsible for the verification of multiple identities should assess whether there are multiple lawful or unlawful identities. Such assessment should be performed where possible in the presence of the third-country national and where necessary by requesting additional clarifications or information. Such assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law.	another EU information system. The authority responsible for the verification of multiple identities should assess whether there are multiple lawful or unlawful identities. Such assessment should be performed where possible in the presence of the third-country national person and where necessary by requesting additional clarifications or information. Such assessment should be performed without delay, in line with legal requirements for the accuracy of information under Union and national law.	
58.	(43) For the links obtained in relation to the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing or vulnerable persons, on persons sought to assist with a judicial procedure, on persons for discreet checks or specific checks	(43) For the links obtained in relation to the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing or vulnerable persons, on persons sought to assist with a judicial procedure, on persons for discreet checks or specific checks	(43) For the links obtained in relation to the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing or vulnerable persons, on persons sought to assist with a judicial procedure, on persons for discreet checks, <i>inquiry checks</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	or on unknown wanted persons, the authority responsible for the verification of multiple identities should be the SIRENE Bureau of the Member State that created the alert. Indeed those categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating the data in one of the other EU information systems. The creation of a link with SIS data should be without prejudice to the actions to be taken in accordance with the [SIS Regulations].	or on unknown wanted persons, the authority responsible for the verification of multiple identities should be the SIRENE Bureau of the Member State that created the alert. Indeed those categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating the data in one of the other EU information systems. The creation of a link with SIS data should be without prejudice to the actions to be taken in accordance with the [SIS Regulations].	or specific checks or on unknown wanted persons, the authority responsible for the verification of multiple identities should be the SIRENE Bureau of the Member State that created the alert. Indeed those categories of SIS alerts are sensitive and should not necessarily be shared with the authorities creating or updating the data in one of the other EU information systems. The creation of a link with SIS data should be without prejudice to the actions to be taken in accordance with the [SIS Regulations].	
59.		<i>(43a) eu-LISA should develop and manage all interoperability components in such a way as to ensure fast, seamless, efficient, controlled access and full availability of such components with a response time in line with the operational needs of the Member States' authorities.</i>		
60.			<i>(43a) Access to the MID by Member State authorities and</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>EU agencies is not foreseen where a white link exists between data from two or more EU information systems. However, this will not affect the users' access rights. Where it becomes evident when accessing data from two or more EU information systems that a white link was wrongly created, that Member State authority or EU agency should be able to correct the situation and replace the link.</i>	
61.	(44) eu-LISA should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should be responsible to develop a central monitoring capacity for data quality and to produce regular data analysis reports to improve the control of implementation and application by Member States of EU information systems. The common quality indicators should	(44) eu-LISA should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should <i>send out automatic and immediate warnings to the authority entering data if minimum data quality standards are not met. eu-LISA should be responsible for developing</i> develop a central monitoring capacity for data quality and to produce, <i>and for producing</i>	(44) eu-LISA should establish automated data quality control mechanisms and common data quality indicators. eu-LISA should be responsible to develop a central monitoring capacity for data quality and to produce regular data analysis reports to improve the control of implementation and application by Member States of EU information systems. The common quality indicators should	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	include the minimum quality standards to store data in the EU information systems or the interoperability components. The goal of such a data quality standards should be for the EU information systems and interoperability components to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions.	regular data analysis reports to improve the control of implementation and application by Member States of EU Union information systems. The common quality indicators should include the minimum quality standards to store data in the EU Union information systems or the interoperability components. The goal of such a data quality standards should be for the EU Union information systems and interoperability components to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions.	include the minimum quality standards to store data in the EU information systems or the interoperability components. The goal of such a data quality standards should be for the EU information systems and interoperability components to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions.	
62.	(45) The Commission should evaluate eu-LISA quality reports and should issue recommendations to Member States where appropriate. Member States should be responsible for preparing an	(45) The Commission should evaluate eu-LISA quality reports and should issue recommendations to Member States where appropriate. Member States should be responsible for preparing an	(45) The Commission should evaluate eu-LISA quality reports and should issue recommendations to Member States where appropriate. Member States should be responsible for preparing an	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	action plan describing actions to remedy any deficiencies in data quality and should report on its progress regularly.	action plan describing actions to remedy any deficiencies in data quality and should report on its progress regularly.	action plan describing actions to remedy any deficiencies in data quality and should report on its progress regularly.	
63.	(46) The Universal Message Format (UMF) should establish a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs. UMF should define a common vocabulary and logical structures for commonly exchanged information with the objective to facilitate interoperability by enabling the creation and reading of the contents of the exchange in a consistent and semantically equivalent manner.	(46) The Universal Message Format (UMF) should establish a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs. UMF should define a common vocabulary and logical structures for commonly exchanged information with the objective to facilitate <i>of facilitating</i> interoperability by enabling the creation and reading of the contents of the exchange in a consistent and semantically equivalent manner.	(46) The Universal Message Format (UMF) should establish a standard for structured, cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs. UMF should define a common vocabulary and logical structures for commonly exchanged information with the objective to facilitate interoperability by enabling the creation and reading of the contents of the exchange in a consistent and semantically equivalent manner.	
64.			<i>(46a) UMF is not meant as a mandatory, sole or preferred standard for the whole field of Justice and Home Affairs and the diverse solutions deployed by the European Commission, the</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>EU agencies and Member States.</i>	
65.	(47) A central repository for reporting and statistics (CRRS) should be established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes. eu-LISA should establish, implement and host the CRRS in its technical sites containing anonymous statistical data from the above-mentioned systems, the common identity repository, the multiple-identity detector and the shared biometric matching service. The data contained in the CRRS should not enable the identification of individuals. eu-LISA should render the data anonymous and should record such anonymous data in the CRRS. The process for rendering the data anonymous should be automated and no direct access by eu-LISA staff should be granted to any personal data stored in the EU information	(47) A central repository for reporting and statistics (CRRS) should be established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes <i>in line with the objectives of the underlying systems and in conformity with their respective legal bases.</i> eu-LISA should establish, implement and host the CRRS in its technical sites containing anonymous statistical data from the above-mentioned systems, the common identity repository <i>CIR</i> , the multiple-identity detector <i>MID</i> and the shared biometric matching service <i>BMS</i> . The data contained in the CRRS should not enable the identification of individuals. eu-LISA should <i>immediately</i> render the data anonymous and should record <i>only</i> such anonymous <i>anonymised</i> data in the CRRS.	(47) A central repository for reporting and statistics (CRRS) should be established to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes. eu-LISA should establish, implement and host the CRRS in its technical sites containing anonymous statistical data from the above-mentioned systems, the common identity repository, the multiple-identity detector and the shared biometric matching service. The data contained in the CRRS should not enable the identification of individuals. eu-LISA should render the data anonymous and should record such anonymous data in the CRRS. The process for rendering the data anonymous should be automated and no direct access by eu-LISA staff should be granted to any personal data stored in the EU information systems or in the interoperability	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	systems or in the interoperability components.	The process for rendering the data anonymous should be automated and no direct access by eu-LISA staff should be granted to any personal data stored in the EU Union information systems or in the interoperability components.	components.	
66.	(48) Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation by national authorities unless such processing is carried out by the designated authorities or central access points of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, when Directive (EU) 2016/680 of the European Parliament and of the Council should apply.	(48) Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation by national authorities unless such processing is carried out by the designated authorities or central access points of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, when in which case Directive (EU) 2016/680 of the European Parliament and of the Council should apply.	(48) Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation by national authorities unless such processing is carried out by the designated authorities or central access points of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, when Directive (EU) 2016/680 of the European Parliament and of the Council should apply.	
67.			(48a) <i>Where the processing of personal data by the Member States for the purpose of</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>interoperability is carried out by the competent authorities for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, Directive (EU) 2016/680 applies.</i> ⁵²	
68.	(49) The specific provisions on data protection of [the EES Regulation], Regulation (EC) No 767/2008, [the ETIAS Regulation] and [the Regulation on SIS in the field of border checks] should apply to the processing of personal data in those respective systems.	(49) The specific provisions on data protection of [the EES Regulation], Regulation (EC) No 767/2008, [the ETIAS Regulation] and [the Regulation on SIS in the field of border checks] should apply to the processing of personal data in those respective systems.	(49) The specific provisions on data protection of the EES Regulation (EU) 2017/2226 , Regulation (EC) No 767/2008, [the ETIAS Regulation], and [the Regulation on SIS in the field of border checks] should apply to the processing of personal data in those respective systems.	
69.	(50) Regulation (EC) No 45/2001 of the European Parliament and of the Council ⁵³	(50) Regulation (EC) No 45/2001 of the European Parliament and of the Council ⁵⁴	(50) Regulation (EC) No 45/2001 of the European Parliament and of the Council ⁵⁵	

⁵² The following recital has been included as part of the political agreement in the ETIAS file: "Where the processing of personal data by the Member States for the purpose of assessing applications is carried out by the competent authorities for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, Directive (EU) 2016/680 applies."

⁵³ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	should apply to the processing of personal data by eu-LISA and other institutions and bodies of the Union when carrying out their responsibilities under this Regulation, without prejudice to Regulation (EU) 2016/794, which should apply to the processing of personal data by Europol.	should apply to the processing of personal data by eu-LISA and other institutions and bodies of the Union when carrying out their responsibilities under this Regulation, without prejudice to Regulation (EU) 2016/794, which should apply to the processing of personal data by Europol.	<i>[Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]</i> should apply to the processing of personal data by eu-LISA and other institutions and bodies of the Union when carrying out their responsibilities under this Regulation, without prejudice to Regulation (EU) 2016/794, which should apply to the processing of personal data by Europol.	
70.	(51) The national supervisory authorities established in	(51) The national supervisory authorities established in	(51) The national supervisory authorities established in	

⁵⁴ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

⁵⁵ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>accordance with [Regulation (EU) 2016/679] should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the processing of personal data by interoperability components.</p>	<p>accordance with {Regulation (EU) 2016/679} <i>or Directive (EU) 2016/680</i> should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the processing of personal data by interoperability components.</p>	<p>accordance with {Regulation (EU) 2016/679} <i>or Directive (EU) 2016/680</i> should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 <i>[Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]</i> should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the processing of</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			personal data by interoperability components.	
71.	(52) "(...) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on ... "	(52) " (...) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 16 April 2018"	(52) " (...) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 16 April 2018 ..."	
72.	(53) Insofar as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS.	(53) Insofar as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS the data accessed through any of the interoperability components .	(53) Insofar as confidentiality is concerned, the relevant provisions of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union should apply to officials or other servants employed and working in connection with SIS.	
73.	(54) Both the Member States and eu-LISA should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues.	(54) Both the Member States and eu-LISA should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues.	(54) Both the Member States and eu-LISA should maintain security plans in order to facilitate the implementation of security obligations and should cooperate with each other in order to address security issues.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	eu-LISA should also make sure there is a continuous use of the latest technological developments to ensure data integrity regarding the development, design and management of the interoperability components.	eu-LISA should also make sure there is a continuous use of the latest technological developments to ensure data integrity regarding the development, design and management of the interoperability components.	eu-LISA should also make sure there is a continuous use of the latest technological developments to ensure data integrity regarding the development, design and management of the interoperability components.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
74.	(55) The implementation of the interoperability components provided for in this Regulation will have an impact on the way checks are carried out at border crossing points. These impacts will result from a combined application of the existing rules of the Regulation (EU) 2016/399 of the European Parliament and of the Council ⁵⁶ and the rules on interoperability provided for in this Regulation.	(55) The implementation of the interoperability components provided for in this Regulation and the integration of the existing national systems and infrastructure with those components will have an impact on the way checks are carried out at border crossing points. These impacts will result from a combined application of the existing rules of the Regulation (EU) 2016/399 of the European Parliament and of the Council ⁵⁷ and the rules on interoperability provided for in this Regulation.	(55) The implementation of the interoperability components provided for in this Regulation will have an impact on the way checks are carried out at border crossing points. These impacts will result from a combined application of the existing rules of the Regulation (EU) 2016/399 of the European Parliament and of the Council ⁵⁸ and the rules on interoperability provided for in this Regulation.	
75.	(56) As a consequence of this combined application of the rules, the European search portal (ESP) should constitute the main access	(56) As a consequence of this combined application of the rules, the European search portal (ESP) should constitute the main access	(56) As a consequence of this combined application of the rules, the European search portal (ESP) should constitute the main access	

⁵⁶ Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders, OJ L 77, 23.3.2016, p.1.

⁵⁷ Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (OJ L 77, 23.3.2016, p. 1).

⁵⁸ Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders, OJ L 77, 23.3.2016, p.1.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<p>point for the compulsory systematic consultation of databases for third-country nationals at border crossing points provided for by the Schengen Borders Code. In addition, the identity data that led to the classification of a link in the multiple-identity detector (MID) as a red link should be taken into account by the border guards for assessing whether or not the person fulfils the conditions of entry defined in the Schengen Borders Code. However the presence of a red link should not in itself constitute a ground for refusal of entry and the existing grounds for refusal of entry listed in the Schengen Borders Code should therefore not be amended.</p>	<p>point for the compulsory systematic consultation of databases for third-country nationals at border crossing points provided for by the Schengen Borders Code. In addition, the identity data that led to the classification of a link in the multiple-identity detector (MID) as a red link should be taken into account by the border guards for assessing whether or not the person fulfils the conditions of entry defined in the Schengen Borders Code. However the presence of a red link should not in itself constitute a ground for refusal of entry and the existing grounds for refusal of entry listed in the Schengen Borders Code should therefore not be amended.</p>	<p>point for the compulsory systematic consultation of databases for third-country nationals persons at border crossing points provided for by the Schengen Borders Code. In addition, the identity data or travel document data that led to the classification of a link in the multiple-identity detector (MID) as a red link should be taken into account by the border guards for assessing whether or not the person fulfils the conditions of entry defined in the Schengen Borders Code. However the presence of a red link should not in itself constitute a ground for refusal of entry and the existing grounds for refusal of entry listed in the Schengen Borders Code should therefore not be amended.</p>	
76.	<p>(57) It would be appropriate to update the Practical Handbook for Border Guards to make these clarifications explicit.</p>	<p>(57) It would be appropriate to update the Practical Handbook for Border Guards to make these clarifications explicit.</p>	<p>(57) It would be appropriate to update the Practical Handbook for Border Guards to make these clarifications explicit.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
77.	(58) However, an amendment of Regulation (EU) 2016/399 would be required in order to add the obligation for the border guard to refer a third-country national to second-line check in case the consultation of the multiple-identity detector (MID) through the European search portal (ESP) would indicate the existence of a yellow link or a red link, in view of not prolonging the waiting time in the first-line checks.	(58) However, an amendment of Regulation (EU) 2016/399 would be required in order to add the obligation for the border guard to refer a third-country national to second-line check in case the consultation of the multiple-identity detector (MID) through the European search portal (ESP) would indicate the existence of a yellow link or a red link, in view of not prolonging the waiting time in the first-line checks.	(58) However, an amendment of Regulation (EU) 2016/399 would be required in order to add the obligation for the border guard to refer a third-country national to second-line check in case the consultation of the multiple-identity detector (MID) through the European search portal (ESP) would indicate the existence of a yellow link or a red link, in view of not prolonging the waiting time in the first-line checks.	
78.	(59) Should the query of the multiple-identity detector (MID) through the European search portal (ESP) result in a yellow link or detect a red link, the border guard on second line should consult the common identity repository or the Schengen Information System or both in order to assess the information on the person being checked, to manually verify his/her different identity and to adapt the colour of the link if	(59) Should the query of the multiple-identity detector (MID) through the European search portal (ESP) result in a yellow link or detect a red link, the border guard on second line should consult the common identity repository CIR or the Schengen Information System SIS or both in order to assess the information on the person being checked, to manually verify his/her different identity and to adapt the colour of the link if	(59) Should the query of the multiple-identity detector (MID) through the European search portal (ESP) result in a yellow link or detect a red link, the border guard on second line should consult the common identity repository or the Schengen Information System or both in order to assess the information on the person being checked, to manually verify his/her different identity and to adapt the colour of the link if	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	required.	required.	required.	
79.	(60) To support the purposes of statistics and reporting, it is necessary to grant access to authorised staff of the competent authorities, institutions and bodies identified in this Regulation to consult certain data related to certain interoperability components without enabling individual identification.	(60) To support the purposes of statistics and reporting, it is necessary to grant access to authorised staff of the competent authorities, institutions and bodies identified in this Regulation to consult certain data related to certain interoperability components without enabling individual identification.	(60) To support the purposes of statistics and reporting, it is necessary to grant access to authorised staff of the competent authorities, institutions and agencies bodies identified in this Regulation to consult certain data related to certain interoperability components without enabling individual identification.	
80.	(61) In order to allow competent authorities and the EU bodies to adapt to the new requirements on the use of the European search portal (ESP), it is necessary to provide for a transitional period. Similarly, in order to allow for the coherent and optimal functioning of the multiple-identity detector (MID), transitional measures should be established for the start of its operations.	(61) In order to allow competent authorities and the Union EU bodies to adapt to the new requirements on the use of the European search portal (ESP) , it is necessary to provide for a transitional period which should entail, inter alia, training programmes for end users so as to ensure that the new instruments operate to their full potential . Similarly, in order to allow for the coherent and optimal functioning of the multiple-identity detector (MID) , transitional measures should be	(61) In order to allow competent authorities and the EU agencies bodies to adapt to the new requirements on the use of the European search portal (ESP), it is necessary to provide for a transitional period. Similarly, in order to allow for the coherent and optimal functioning of the multiple-identity detector (MID), transitional measures should be established for the start of its operations.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		established for the start of its operations.		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
81.	(62) The costs for the development of the interoperability components projected under the current Multiannual Financial Framework are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council ⁵⁹ . Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should reallocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.	(62) The costs for the development of the interoperability components projected under the current Multiannual Financial Framework are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council⁶⁰ <i>should be reallocated to</i> . Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should reallocate the amount currently attributed. <i>In addition, eu-LISA should endeavour to keep costs to a minimum and to identify and implement the most cost-effective technical solutions.</i>	(62) The costs for the development of the interoperability components projected under the current Multiannual Financial Framework are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council ⁶¹ . Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should reallocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.	

⁵⁹ Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

⁶⁰ Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

⁶¹ Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
82.		<i>(62a) It would be appropriate that, during the development phase of the interoperability components, the Commission assess the necessity of further harmonisation of national systems and infrastructure of Member States at external borders and makes recommendations. Those recommendations should also include an impact assessment and an assessment of the cost for the Union budget.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
83.	(63) In order to supplement certain detailed technical aspects of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of the profiles for the users of the European search portal (ESP) and the content and format of the ESP replies. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 ⁶² . In particular, to ensure equal participation in the preparation of delegated acts, the European	(63) In order to supplement certain detailed technical aspects of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. <i>In particular, power should be delegated to the Commission</i> in respect of the profiles for the users of the European search portal (ESP), and the content and format of the ESP replies, <i>the procedures to determine the cases where identity data can be considered as identical or similar, and the rules on the operation of the CRRS, including specific safeguards for processing of personal data and security rules applicable to the repository.</i> It is of particular importance that the Commission carry out appropriate consultations during	(63) In order to supplement certain detailed technical aspects of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of the <i>extension of the transitional period for the use of the European Search Portal (ESP)</i> profiles for the users of the European search portal (ESP) and the content and format of the ESP replies. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 ⁶⁴ . In	

⁶² http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

⁶⁴ http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Parliament and the Council should receive all documents at the same time as Member State experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 ⁶³ . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member State experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member State experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.	
84.	(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on: automated data quality control mechanisms, procedures	(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on: automated data quality control mechanisms, procedures	(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on: <i>technical details of profiles for the users of the</i>	

⁶³ http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.123.01.0001.01.ENG.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<p>and indicators; development of the UMF standard; procedures for determining cases of similarity of identities; the operation of the central repository for reporting and statistics; and cooperation procedure in case of security incidents. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council⁶⁵.</p>	<p>and indicators; development of the UMF standard; procedures for determining cases of similarity of identities; the operation of the central repository for reporting and statistics; and cooperation procedure in case of security incidents. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council⁶⁶.</p>	<p><i>European search portal (ESP); format of the ESP replies; performance requirements and performance monitoring of the shared BMS;</i> automated data quality control mechanisms, procedures and indicators; development of the UMF standard; procedures for determining cases of similarity of identities; the operation of the central repository for reporting and statistics; and cooperation procedure in case of security incidents; <i>and specifications of the technical solution to facilitate the querying of EU information systems and the CIR.</i> Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of</p>	

⁶⁵ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

⁶⁶ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			the European Parliament and of the Council ⁶⁷ .	
85.	(65) Regulation 2016/794 shall apply for any processing of Europol data for the purposes of this Regulation.	(65) Regulation 2016/794 shall apply for any processing of Europol data for the purposes of this Regulation.	(65) Regulation (EU) 2016/794 shall apply for any processing of Europol data for the purposes of this Regulation.	
86.		<i>(65a) As interoperability components will involve the processing of significant amounts of sensitive personal data, it is important that persons whose data is processed through those components can effectively exercise their rights as data subjects as laid down in Regulation (EU) 2016/679, Directive (EU) 680/2016 and Regulation (EC) No 45/2001. In that regard, in the same way as Member State authorities have been provided with a single portal to carry out searches in Union information systems, the data subjects should be provided</i>		

⁶⁷ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>with a single web service through which they can exercise their rights to access to and rectification, erasure and restriction of their personal data. eu-LISA should establish such a web service and host it in its technical site. As eu-LISA is not responsible for the entry of personal data or the verification of identities, any request by a data subject should be transmitted via the web service to either the Member State responsible for the manual verification of different identities or the Member State responsible for the entry of the data into the underlying information system.</i>		
87.		<i>(65b) Article 8(2) of the European Convention on Human Rights states that any interference with the right to respect for private life, must pursue a legitimate aim and must be both necessary and proportionate except in such</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>cases when, in accordance with the law such an action is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.</i>		
88.		<i>(65c) One of the core principles of data protection is data minimisation as highlighted in Article 5(1)(c) of Regulation (EU) 2016/679 in accordance with which the processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.</i>		
89.		<i>(65d) Article 5(1)(b) of Regulation (EU) 2016/679 provides that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>that is incompatible with those purposes. Furthermore, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes must respect the principle of purpose limitation.</i>		
90.			<i>(65a) This Regulation should contain clear provisions on liability and right to compensation for unlawful processing of personal data or from any other act incompatible with it, without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EC) No 45/2001. With regard to the role of eu-LISA as a data processor, this latter should be responsible for the damage it provoked where it has not complied with the specific obligations of this Regulation</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>directed to it, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller.</i>	
91.	(66) This Regulation is without prejudice to the application of Directive 2004/38/EC.	(66) This Regulation is without prejudice to the application of Directive 2004/38/EC.	(66) This Regulation is without prejudice to the application of Directive 2004/38/EC.	
92.	(67) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> .	(67) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> .	(67) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> .	
93.	(68) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen <i>acquis</i> , Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six	(68) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen <i>acquis</i> , Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six	(68) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen <i>acquis</i> , Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	months after the adoption of this Regulation whether it will implement it in its national law.	months after the adoption of this Regulation whether it will implement it in its national law.	months after the adoption of this Regulation whether it will implement it in its national law.	
94.	(69) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC ⁶⁸ ; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.	(69) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC ⁶⁹ ; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.	(69) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC ⁷⁰ ; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.	
95.	(70) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> in which Ireland does not	(70) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> in which Ireland does not	(70) This Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> in which Ireland does not	

⁶⁸ Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

⁶⁹ Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

⁷⁰ Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	take part, in accordance with Council Decision 2002/192/EC ⁷¹ ; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it nor subject to its application.	take part, in accordance with Council Decision 2002/192/EC ⁷² ; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it nor subject to its application.	take part, in accordance with Council Decision 2002/192/EC ⁷³ ; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it nor subject to its application.	
96.	(71) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and	(71) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and	(71) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and	

⁷¹ Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis (OJ L 64, 7.3.2002, p. 20).

⁷² Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis (OJ L 64, 7.3.2002, p. 20).

⁷³ Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis (OJ L 64, 7.3.2002, p. 20).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	development of the Schengen acquis ⁷⁴ which fall within the area referred to in Article 1, points A, B and G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement ⁷⁵ .	development of the Schengen acquis ⁷⁶ which fall within the area referred to in Article 1, points A, B and G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement ⁷⁷ .	development of the Schengen acquis ⁷⁸ which fall within the area referred to in Article 1, points A, B and G of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement ⁷⁹ .	

⁷⁴ OJ L 176, 10.7.1999, p. 36.

⁷⁵ OJ L 176, 10.7.1999, p. 31.

⁷⁶ OJ L 176, 10.7.1999, p. 36.

⁷⁷ OJ L 176, 10.7.1999, p. 31.

⁷⁸ OJ L 176, 10.7.1999, p. 36.

⁷⁹ OJ L 176, 10.7.1999, p. 31.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
97.	(72) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis ⁸⁰ which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC ⁸¹ .	(72) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis ⁸² which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC ⁸³ .	(72) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis ⁸⁴ which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC ⁸⁵ .	

⁸⁰ OJ L 53, 27.2.2008, p. 52.

⁸¹ OJ L 53, 27.2.2008, p. 1.

⁸² OJ L 53, 27.2.2008, p. 52.

⁸³ OJ L 53, 27.2.2008, p. 1.

⁸⁴ OJ L 53, 27.2.2008, p. 52.

⁸⁵ OJ L 53, 27.2.2008, p. 1.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
98.	(73) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> within the meaning of the Protocol between the European Union, 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 Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen <i>acquis</i> ⁸⁶ which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ⁸⁷ .	(73) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> within the meaning of the Protocol between the European Union, 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 Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen <i>acquis</i> ⁸⁸ which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ⁸⁹ .	(73) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen <i>acquis</i> within the meaning of the Protocol between the European Union, 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 Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen <i>acquis</i> ⁹⁰ which fall within the area referred to in Article 1, points A, B and G of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ⁹¹ .	

⁸⁶ OJ L 160, 18.6.2011, p. 21.

⁸⁷ OJ L 160, 18.6.2011, p. 19.

⁸⁸ OJ L 160, 18.6.2011, p. 21.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
99.	(74) As regards Cyprus, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 3(2) of the 2003 Act of Accession.	(74) As regards Cyprus, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 3(2) of the 2003 Act of Accession.	(74) As regards Cyprus, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 3(2) of the 2003 Act of Accession.	
100	(75) As regards Bulgaria and Romania, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2005 Act of Accession read in conjunction with Council Decision 2010/365/EU ⁹² and Council Decision (EU) 2017/1908 ⁹³ .	(75) As regards Bulgaria and Romania, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2005 Act of Accession read in conjunction with Council Decision 2010/365/EU ⁹⁴ and Council Decision (EU) 2017/1908 ⁹⁵ .	(75) As regards Bulgaria and Romania, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2005 Act of Accession read in conjunction with Council Decision 2010/365/EU ⁹⁶ and Council Decision (EU) 2017/1908 ⁹⁷ , and Council	

⁸⁹ OJ L 160, 18.6.2011, p. 19.

⁹⁰ OJ L 160, 18.6.2011, p. 21.

⁹¹ OJ L 160, 18.6.2011, p. 19.

⁹² Council Decision 2010/365/EU of 29 June 2010 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Bulgaria and Romania, OJ L 166, 1.7.2010, p. 17.

⁹³ Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania, OJ M 269, 19.10.2017, p. 39.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>Decision (EU) 2018/934⁹⁸.</i>	
101	(76) As regards Croatia, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2011 Act of Accession read in conjunction with Council Decision (EU) 2017/733 ⁹⁹ .	(76) As regards Croatia, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2011 Act of Accession read in conjunction with Council Decision (EU) 2017/733 ¹⁰⁰ .	(76) As regards Croatia, the provisions related to the SIS and the VIS constitute provisions building upon, or otherwise related to, the Schengen acquis within the meaning of Article 4(2) of the 2011 Act of Accession read in conjunction with Council Decision (EU) 2017/733 ¹⁰¹ .	

⁹⁴ Council Decision 2010/365/EU of 29 June 2010 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Bulgaria and Romania, OJ L 166, 1.7.2010, p. 17.

⁹⁵ Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania, OJ M 269, 19.10.2017, p. 39.

⁹⁶ Council Decision 2010/365/EU of 29 June 2010 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Bulgaria and Romania, OJ L 166, 1.7.2010, p. 17.

⁹⁷ Council Decision (EU) 2017/1908 of 12 October 2017 on the putting into effect of certain provisions of the Schengen acquis relating to the Visa Information System in the Republic of Bulgaria and Romania, OJ M 269, 19.10.2017, p. 39.

⁹⁸ Council Decision (EU) 2018/934 of 25 June 2018 on the putting into effect of the remaining provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania, OJ L 165, 2.7.2018, p. 37.

⁹⁹ Council Decision (EU) 2017/733 of 25 April 2017 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Croatia, OJ L 108, 26.4.2017, p. 31.

¹⁰⁰ Council Decision (EU) 2017/733 of 25 April 2017 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Croatia, OJ L 108, 26.4.2017, p. 31.

¹⁰¹ Council Decision (EU) 2017/733 of 25 April 2017 on the application of the provisions of the Schengen acquis relating to the Schengen information System in the Republic of Croatia, OJ L 108, 26.4.2017, p. 31.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
102	(77) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and shall be applied in accordance with those rights and principles.	(77) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and shall be applied in accordance with those rights and principles.	(77) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and should shall be applied in accordance with those rights and principles.	
103	(78) In order to have this Regulation fit into the existing legal framework, the Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Council Decision 2008/633/JHA, Regulation (EC) 767/2008 and Council Decision 2004/512/EC should be amended accordingly,	(78) In order to have this Regulation fit into the existing legal framework, the Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Council Decision 2008/633/JHA, Regulation (EC) 767/2008 and Council Decision 2004/512/EC should be amended accordingly,	(78) In order to have this Regulation fit into the existing legal framework, the Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Council Decision 2008/633/JHA, Regulation (EC) No 767/2008 and Council Decision 2004/512/EC should be amended accordingly,	
104	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
105	CHAPTER I General provisions	CHAPTER I General provisions	CHAPTER I General provisions	
106	<i>Article 1 Subject matter</i>	<i>Article 1 Subject matter</i>	<i>Article 1 Subject matter</i>	
107	1. This Regulation, together with [Regulation 2018/xx on interoperability police and judicial cooperation, asylum and migration], establishes a framework to ensure the interoperability between the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and [the European Criminal Records Information System for third-country nationals (ECRIS-TCN)] in order for those systems and data to supplement each other.	1. This Regulation, together with [Regulation 2018/xx on interoperability police and judicial cooperation, asylum and migration], establishes a framework to ensure the interoperability between the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and [the European Criminal Records Information System for third-country nationals (ECRIS-TCN)] in order for those systems and data to supplement each other.	1. This Regulation, together with [Regulation 2018/xx on interoperability police and judicial cooperation, asylum and migration], establishes a framework to ensure the interoperability between the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)], Eurodac, the Schengen Information System (SIS), and [the European Criminal Records Information System for third-country nationals (ECRIS-TCN)] in order for those systems and data to supplement each other.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
108	2. The framework shall include the following interoperability components:	2. The framework shall include the following interoperability components:	2. The framework shall include the following interoperability components:	
109	(a) a European search portal (ESP);	(a) a European search portal (ESP);	(a) a European search portal (ESP);	
110	(b) a shared biometric matching service (shared BMS);	(b) a shared biometric matching service (shared BMS);	(b) a shared biometric matching service (shared BMS);	
111	(c) a common identity repository (CIR);	(c) a common identity repository (CIR);	(c) a common identity repository (CIR);	
112	(d) a multiple-identity detector (MID).	(d) a multiple-identity detector (MID).	(d) a multiple-identity detector (MID).	
113	3. This Regulation also lays down provisions on data quality requirements, on a Universal Message Format (UMF), on a central repository for reporting and statistics (CRRS) and lays down the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), with respect to the design and operation of the interoperability components.	3. This Regulation also lays down provisions on data quality requirements, on a Universal Message Format (UMF), on a central repository for reporting and statistics (CRRS) and lays down the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), with respect to the design, <i>development</i> and operation of the interoperability components.	3. This Regulation also lays down provisions on data quality requirements, on a Universal Message Format (UMF), on a central repository for reporting and statistics (CRRS) and lays down the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), with respect to the design and operation of the interoperability components.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
114	<p>4. This Regulation also adapts the procedures and conditions for Member State law enforcement authorities and for the European Union Agency for Law Enforcement Cooperation (Europol) access to the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS),] and Eurodac for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence.</p>	<p>4. This Regulation also adapts the procedures and conditions for Member State law enforcement <i>designated</i> authorities and for the European Union Agency for Law Enforcement Cooperation (Europol) access to the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS),] and Eurodac for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence.</p>	<p>4. This Regulation also adapts the procedures and conditions for Member State law enforcement <i>designated</i> authorities and for the European Union Agency for Law Enforcement Cooperation (Europol) access to the Entry/Exit System (EES), the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS),] and Eurodac for the purposes of the prevention, detection and or investigation of terrorist offences or of other serious criminal offences falling under their competence.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
115		<i>4a. This Regulation also lays down a framework for verifying identities of third-country nationals and for identifying third-country nationals.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
116	<i>Article 2 Objectives of interoperability</i>	<i>Article 2 Objectives of interoperability</i>	<i>Article 2 Objectives of interoperability</i>	
117	1. By ensuring interoperability, this Regulation shall have the following objectives:	1. By ensuring interoperability, this Regulation shall have the following objectives:	1. By ensuring interoperability, this Regulation shall have has the following objectives:	
118	(a) to improve the management of the external borders;	(a) to improve the management of enhance the effectiveness and efficiency of border checks at the external borders;	(a) to improve the effectiveness and efficiency of checks at the external borders; management of the external borders;	
119	(b) to contribute to preventing and combating irregular migration;	(b) to contribute to preventing and combating tackling irregular migration;	(b) to contribute to preventing and combating irregular illegal immigration;	
120	(c) to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States;	(c) to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States;	(c) to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding the security in the territories of the Member States;	
121	(d) to improve the implementation of the common	(d) to improve the implementation of the common	(d) to improve the implementation of the common	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	visa policy; and	visa policy; and	visa policy; and	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
122	(e) to assist in examining application for international protection.	(e) to assist in examining application for international protection.	(e) to assist in examining applications for international protection <i>lodged in a Member State</i> ;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
123		<i>(ea) to contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences;</i>		
124		<i>(eb) to aid in the identification of unknown persons who are unable to identify themselves or unidentified human remains in cases of natural disasters, accidents or terrorist attacks.</i>		
125			<i>(f) in the event of a natural disaster or an accident, for humanitarian reasons, to assist in the identification of unknown persons who are not able to identify themselves or unidentified human remains.</i>	
126	2. The objectives of ensuring interoperability shall be achieved by:	2. The Those objectives of ensuring interoperability shall be achieved by:	2. The objectives of ensuring interoperability referred to in paragraph 1 shall be achieved in particular by:	
127	(a) ensuring the correct identification of persons;	(a) ensuring facilitating the correct identification of persons third-country nationals registered in the Union	(a) ensuring the correct identification of persons;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>information systems;</i>		
128	(b) contributing to fighting identity fraud;	(b) contributing to fighting <i>combating</i> identity fraud;	(b) contributing to fighting identity fraud;	
129	(c) improving and harmonising data quality requirements of the respective EU information systems;	(c) improving <i>the data quality</i> and harmonising data <i>the</i> quality requirements of <i>for</i> the respective EU <i>data stored in the Union</i> information systems <i>while respecting the data processing requirements of the legal bases of the individual systems, data protection standards and principles;</i>	(c) improving and harmonising data quality requirements of the respective EU information systems <i>while respecting the data processing requirements of the legal bases of the individual systems, data protection standards and principles;</i>	
130		(ca) <i>improving judicial cooperation in the area of freedom, security and justice;</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
131	(d) facilitating the technical and operational implementation by Member States of existing and future EU information systems;	(d) facilitating the technical and operational implementation by Member States of existing and future EU Union information systems;	(d) facilitating and supporting the technical and operational implementation by Member States of existing and future EU information systems;	
132	(e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems;	(e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU Union information systems, without prejudice to the special protection and safeguards afforded to certain categories of data ;	(e) strengthening and simplifying and making more uniform the data security and data protection conditions that govern the respective EU information systems, without prejudice to the special protection and safeguards afforded to certain categories of data ;	
133	(f) streamlining the conditions for law enforcement access to the EES, the VIS, [the ETIAS] and Eurodac;	(f) streamlining the and simplifying the conditions for designated authorities' access to the EES, VIS, [ETIAS] and Eurodac, while ensuring the necessary and proportionate conditions for law enforcement access to the EES, the VIS, [the ETIAS] and Eurodac ;	(f) streamlining the conditions for law enforcement access by designated authorities to the EES, the VIS, [the ETIAS] and Eurodac;	
134	(g) supporting the purposes of the EES, the VIS, [the ETIAS],	(g) supporting the purposes of the EES, the VIS, [the ETIAS],	(g) supporting the purposes of the EES, the VIS, [the ETIAS],	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Eurodac, the SIS and [the ECRIS-TCN system].	Eurodac, the SIS and [the ECRIS-TCN system].	Eurodac, the SIS and [the ECRIS-TCN system].	
135	<i>Article 3 Scope</i>	<i>Article 3 Scope</i>	<i>Article 3 Scope</i>	
136	1. This Regulation applies to [the Entry/Exit System (EES)], the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)] and the Schengen Information System (SIS).	1. This Regulation applies to [the Entry/Exit System (EES)], the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)] and the Schengen Information System (SIS).	1. This Regulation applies to [the Entry/Exit System (EES)], the Visa Information System (VIS), [the European Travel Information and Authorisation System (ETIAS)] and the Schengen Information System (SIS).	
137	2. This Regulation applies to persons in respect of whom personal data may be processed in the EU information systems referred to in paragraph 1.	2. This Regulation applies to persons in respect of whom personal data may be processed in the EU Union information systems referred to in paragraph 1, <i>only for the purposes as defined in the underlying legal basis for those information systems.</i>	2. This Regulation applies to persons in respect of whom personal data may be processed in the EU information systems referred to in paragraph 1.	
138	<i>Article 4 Definitions</i>	<i>Article 4 Definitions</i>	<i>Article 4 Definitions</i>	
139	For the purposes of this Regulation, the following	For the purposes of this Regulation, the following	For the purposes of this Regulation, the following	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	definitions apply:	definitions apply:	definitions apply:	
140	(1) ‘external borders’ means external borders as defined in Article 2(2) of Regulation (EU) 2016/399;	(1) ‘external borders’ means external borders as defined in Article 2(2) of Regulation (EU) 2016/399;	(1) ‘external borders’ means external borders as defined in Article 2(2) of Regulation (EU) 2016/399;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
141	(2) ‘border checks’ means border checks as defined in Article 2(11) of Regulation (EU) 2016/399;	(2) ‘border checks’ means border checks as defined in Article 2(11) of Regulation (EU) 2016/399;	(2) ‘border checks’ means border checks as defined in Article 2(11) of Regulation (EU) 2016/399;	
142	(3) ‘border authority’ means the border guard assigned in accordance with national law to carry out border checks;	(3) ‘border authority’ means the border guard assigned in accordance with national law to carry out border checks <i>as defined in Article 2(11) of Regulation (EU) 2016/399</i> ;	(3) ‘border authority’ means the border guard assigned in accordance with national law to carry out border checks <i>as defined in point 11 of Article 2 of Regulation (EU) 2016/399</i> ;	
143	(4) ‘supervisory authorities’ means the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680;	(4) ‘supervisory authorities’ means the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680;	(4) ‘supervisory authorities’ means the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and the supervisory authority established in accordance with Article 41(1) of Directive (EU) 2016/680;	
144	(5) ‘verification’ means the process of comparing sets of data to establish the validity of a claimed identity (one-to-one check);	(5) ‘verification’ means the process of comparing sets of data to establish the validity of a claimed identity (one-to-one check);	(5) ‘verification’ means the process of comparing sets of data to establish the validity of a claimed identity (one-to-one check);	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
145	(6) ‘identification’ means the process of determining a person’s identity through a database search against multiple sets of data (one-to-many check);	(6) ‘identification’ means the process of determining a person’s identity through a database search against multiple sets of data (one-to-many check);	(6) ‘identification’ means the process of determining a person’s identity through a database search against multiple sets of data (one-to-many check);	
146	(7) ‘third-country national’ means a person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty, or a stateless person or a person whose nationality is unknown;	(7) ‘third-country national’ means a person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty, or a stateless person or a person whose nationality is unknown;	(7) ‘third-country national’ means a person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty, or a stateless person or a person whose nationality is unknown;	
147	(8) ‘alphanumeric data’ means data represented by letters, digits, special characters, spaces and punctuation marks;	(8) ‘alphanumeric data’ means data represented by letters, digits, special characters, spaces and punctuation marks;	(8) ‘alphanumeric data’ means data represented by letters, digits, special characters, spaces and punctuation marks;	
148	(9) ‘identity data’ means the data referred to in Article 27(3)(a) to (h);	(9) ‘identity data’ means the data referred to in Article 27(3)(a) to (h);	(9) ‘identity data’ means the data referred to in Article 27(3)(a) to (h);	
149	(10) ‘fingerprint data’ means the data relating to the fingerprints of an individual;	(10) ‘fingerprint data’ means the data relating to the fingerprints of an individual;	(10) <i>‘dactyloscopic data’ means fingerprints images, images of fingerprint latents,</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>palm prints, and palm prints latents¹⁰² which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;</i> ‘fingerprint data’ means the data relating to the fingerprints of an individual;	
150	(11) ‘facial image’ means digital images of the face;	(11) ‘facial image’ means digital images of the face;	(11) ‘facial image’ means digital images of the face;	
151	(12) ‘biometric data’ means fingerprint data and/or facial image;	(12) ‘biometric data’ means fingerprint data and/or facial image;	(12) ‘biometric data’ means fingerprint <i>dactyloscopic</i> data and/or facial image;	
152	(13) ‘biometric template’ means a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications;	(13) ‘biometric template’ means a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications;	(13) ‘biometric template’ means a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications;	
153	(14) ‘travel document’ means a passport or other equivalent document entitling the holder to	(14) ‘travel document’ means a passport or other equivalent document entitling the holder to	(14) ‘travel document’ means a passport or other equivalent document entitling the holder to	

¹⁰² NB: Same definition as in Council Decision 2008/616/JHA.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	cross the external borders and to which a visa may be affixed;	cross the external borders and to which a visa may be affixed;	cross the external borders and to which a visa may be affixed;	
154	(15) ‘travel document data’ means the type, number and country of issuance of the travel document, the date of expiry of the validity of the travel document and the three-letter code of the country issuing the travel document;	(15) ‘travel document data’ means the type, number and country of issuance of the travel document, the date of expiry of the validity of the travel document and the three-letter code of the country issuing the travel document;	(15) ‘travel document data’ means the type, number and country of issuance of the travel document, the date of expiry of the validity of the travel document and the three-letter code of the country issuing the travel document;	
155	(16) ‘travel authorisation’ means travel authorisation as defined in Article 3 of the [ETIAS Regulation];	(16) ‘travel authorisation’ means travel authorisation as defined in Article 3 of the [ETIAS Regulation];	(16) ‘travel authorisation’ means travel authorisation as defined in Article 3 of the [ETIAS Regulation];	
156	(17) ‘short-stay visa’ means visa as defined in Article 2(2)(a) of Regulation (EC) No 810/2009;	(17) ‘short-stay visa’ means visa as defined in Article 2(2)(a) of Regulation (EC) No 810/2009;	(17) ‘short-stay visa’ means visa as defined in Article 2(2)(a) of Regulation (EC) No 810/2009;	
157	(18) ‘EU information systems’ means the large-scale IT systems managed by eu-LISA;	(18) ‘ EU Union information systems’ means the large-scale IT systems EES, VIS, [ETIAS], Eurodac, SIS and [ECRIS-TCN] operationally managed by eu-LISA;	(18) ‘EU information systems’ means the large-scale IT systems operationally managed by eu-LISA;	
158	(19) ‘Europol data’ means personal data provided to Europol	(19) ‘Europol data’ means personal data processed by	(19) ‘Europol data’ means personal data processed by	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	for the purpose referred to in Article 18(2)(a) of Regulation (EU) 2016/794;	provided to Europol for the purpose purposes referred to in Article 18(2)(a), (b) and (c) of Regulation (EU) 2016/794;	provided to Europol for the purpose referred to in Article 18(2)(a) to (c) of Regulation (EU) 2016/794;	
159	(20) ‘Interpol databases’ means the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN);	(20) ‘Interpol databases’ means the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN);	(20) ‘Interpol databases’ means the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (Interpol TDAWN);	
160	(21) ‘match’ means the existence of a correspondence established by comparing two or more occurrences of personal data recorded or being recorded in an information system or database;	(21) ‘match’ means the existence of a same or similar correspondence as a result of an automated comparison between established by comparing two or more occurrences of personal data recorded or being recorded in an information system or database;	(21) ‘match’ means the existence of a correspondence as a result of an automated comparison between established by comparing two or more occurrences of personal data recorded or being recorded in an information system or database;	
161	(22) ‘hit’ means the confirmation of one match or several matches;	(22) ‘hit’ means the confirmation of one match or several matches;	(22) ‘hit’ means the confirmation of one match or several matches;	
162	(23) ‘police authority’ means ‘competent authority’ as defined in Article 3(7) of Directive	(23) ‘police authority’ means ‘competent authority’ as defined in Article 3(7) of Directive	(23) ‘police authority’ means ‘competent authority’ as defined in Article 3(7) of Directive (EU)	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	2016/680;	2016/680;	2016/680;	
163	(24) ‘designated authorities’ means the Member State designated authorities referred to in Article 29(1) of Regulation (EU) 2017/2226, Article 3(1) of Council Decision 2008/633/JHA, [Article 43 of the ETIAS Regulation] and [Article 6 of the Eurodac Regulation];	(24) ‘designated authorities’ means the Member State designated authorities referred to as defined in Article 29(1) 3(26) of Regulation (EU) 2017/2226, Article 3(1) 2(1)(d) of Council Decision 2008/633/JHA, [Article 3(21) of the ETIAS Regulation] and referred to in [Article 6 of the Eurodac Regulation];	(24) ‘designated authorities’ means the Member State designated authorities referred to in Article 29(1) of Regulation (EU) 2017/2226, Article 3(1) of Council Decision 2008/633/JHA, [Article 43 50 of the ETIAS Regulation] and [Article 6 of the Eurodac Regulation];	
164	(25) ‘terrorist offence’ means an offence under national law which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541;	(25) ‘terrorist offence’ means an offence under national law which corresponds or is equivalent to one of the offences referred to in Articles 3 to 14 of Directive (EU) 2017/541, or which is equivalent to one of those offences for the Member States which are not bound by that Directive;	(25) ‘terrorist offence’ means an offence under national law which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541;	
165	(26) ‘serious criminal offence’ means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Framework	(26) ‘serious criminal offence’ means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Framework	(26) ‘serious criminal offence’ means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Framework	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Decision 2002/584/JHA, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;	Decision 2002/584/JHA, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;	Decision 2002/584/JHA, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years;	
166	(27) 'EES' means the Entry/Exit System as referred to in Regulation (EU) 2017/2226;	(27) 'EES' means the Entry/Exit System as referred to in Regulation (EU) 2017/2226;	(27) 'Entry/Exit System' ('EES') means the Entry/Exit System as referred to in Regulation (EU) 2017/2226;	
167	(28) 'VIS' means the Visa Information System as referred to in Regulation (EC) No 767/2008;	(28) 'VIS' means the Visa Information System as referred to in Regulation (EC) No 767/2008;	(28) 'Visa Information System' ('VIS') means the Visa Information System as referred to in Regulation (EC) No 767/2008;	
168	(29) ['ETIAS' means the European Travel Information and Authorisation System as referred to in the ETIAS Regulation];	(29) ['ETIAS' means the European Travel Information and Authorisation System as referred to in the ETIAS Regulation];	(29) [<i>the European Travel Information and Authorisation System</i>] ('ETIAS') means the European Travel Information and Authorisation System as referred to in the ETIAS Regulation];	
169	(30) 'Eurodac' means Eurodac as referred to in the [Eurodac Regulation];	(30) 'Eurodac' means Eurodac as referred to in the [Eurodac Regulation];	(30) 'Eurodac' means Eurodac as referred to in the [Eurodac Regulation];	
170	(31) 'SIS' means the Schengen Information System as referred to [in the Regulation on SIS in the	(31) 'SIS' means the Schengen Information System as referred to [in the Regulation on SIS in the	(31) 'Schengen Information System' ('SIS') means the Schengen Information System as	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	field of border checks, Regulation on SIS in the field of law enforcement and Regulation on SIS in the field of illegal return];	field of border checks, Regulation on SIS in the field of law enforcement and Regulation on SIS in the field of illegal return]; <i>(Horizontal amendment applies throughout the text.)</i>	referred to [in the Regulation on SIS in the field of border checks, Regulation on SIS in the field of law enforcement <i>police cooperation and judicial cooperation in criminal matters</i> and Regulation on SIS <i>for the return of illegally staying third-country nationals</i> in the field of illegal return];	
171	(32) ['ECRIS-TCN System' means the European Criminal Records Information System holding conviction information on third-country national and stateless persons as referred to in the ECRIS-TCN System Regulation];	(32) ['ECRIS-TCN System' means the European Criminal Records Information System holding conviction information on third-country national and stateless persons as referred to in the ECRIS-TCN System Regulation];	(32) ['ECRIS-TCN System' means the European Criminal Records Information System <i>the centralised system for the identification of Member States</i> holding conviction information on third-country nationals and stateless persons as referred to in the ECRIS-TCN System Regulation];	
172	(33) 'ESP' means the European search portal as referred to in Article 6;	(33) 'ESP' means the European search portal as referred to in Article 6;	(33) 'ESP' means the European search portal as referred to in Article 6;	
173	(34) 'shared BMS' means the shared biometric matching service as referred to in Article	(34) 'shared BMS' means the shared biometric matching service as referred to in Article	(34) 'shared BMS' means the shared biometric matching service as referred to in Article	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	15;	15;	15;	
174	(35) 'CIR' means the common identity repository as referred to in Article 17;	(35) 'CIR' means the common identity repository as referred to in Article 17;	(35) 'CIR' means the common identity repository as referred to in Article 17;	
175	(36) 'MID' means the multiple-identity detector as referred to in Article 25;	(36) 'MID' means the multiple-identity detector as referred to in Article 25;	(36) 'MID' means the multiple-identity detector as referred to in Article 25;	
176	(37) 'CRRS' means the central repository for reporting and statistics as referred to in Article 39.	(37) 'CRRS' means the central repository for reporting and statistics as referred to in Article 39.	(37) 'CRRS' means the central repository for reporting and statistics as referred to in Article 39.	
177	<i>Article 5 Non-discrimination</i>	<i>Article 5 Non-discrimination and fundamental rights</i>	<i>Article 5 Non-discrimination</i>	
178	Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. It shall fully respect human dignity and integrity. Particular attention shall be paid to children, the elderly and	Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as sex, racial or <i>race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth</i> , disability, age or sexual	Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as <i>gender</i> sex , racial or ethnic origin, religion or belief, disability, age or sexual orientation. It shall fully respect human dignity and integrity. Particular attention shall be paid to children, the elderly and	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	persons with a disability.	orientation. It shall fully respect human dignity and integrity <i>and fundamental rights, including the right to respect for one's private life and to the protection of personal data</i> . Particular attention shall be paid to children, the elderly and persons with a disability <i>and persons in need of international protection. The best interests of the child shall be a primary consideration.</i>	persons with a disability.	
179		<i>One year after the date of entry into force of this Regulation, the Commission shall conduct an ex-post evaluation aimed at assessing the impact of interoperability on the right to non-discrimination.</i>		
180	CHAPTER II European Search Portal	CHAPTER II European Search Portal	CHAPTER II European Search Portal	
181	<i>Article 6 European search portal</i>	<i>Article 6 European search portal</i>	<i>Article 6 European search portal</i>	
182	1. A European search portal	1. A European search portal	1. A European search portal	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>(ESP) is established for the purposes of ensuring that Member State authorities and EU bodies have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases that they need to perform their tasks in accordance with their access rights and of supporting the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] and the Europol data.</p>	<p>(ESP) is established for the purposes of ensuring that facilitating the controlled access of Member State authorities and EU bodies have fast, seamless, efficient, systematic and controlled access Union agencies to the EU Union information systems, to the Europol data and the Interpol databases that they need to perform for the performance of their tasks and in accordance with their access rights and of supporting the objectives and purposes of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] and the Europol data as well as in accordance with Regulation (EU) 2016/679, while fully respecting the principles of necessity and proportionality.</p>	<p>(ESP) is established for the purposes of ensuring that Member State authorities and EU bodies agencies have fast, seamless, efficient, systematic and controlled access to the EU information systems, the Europol data and the Interpol databases that they need to perform their tasks in accordance with their access rights and of supporting the objectives of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] and the Europol data.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
183	2. The ESP shall be composed of:	2. The ESP shall be composed of:	2. The ESP shall be composed of:	
184	(a) a central infrastructure, including a search portal enabling the simultaneous querying of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] as well as of the Europol data and the Interpol databases;	(a) a central infrastructure, including a search portal enabling the simultaneous querying of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] as well as of the Europol data and the Interpol databases;	(a) a central infrastructure, including a <i>technical</i> search portal enabling the simultaneous querying of the EES, the VIS, [the ETIAS], Eurodac, the SIS, [the ECRIS-TCN system] as well as of the Europol data and the Interpol databases;	
185	(b) a secure communication channel between the ESP, Member States and EU bodies that are entitled to use the ESP in accordance with Union law;	(b) a secure communication channel between the ESP, Member States and EU bodies <i>Union agencies</i> that are entitled to use the ESP in accordance with Union law ;	(b) a secure communication channel between the ESP, Member States and EU <i>agencies</i> bodies that are entitled to use the ESP in accordance with Union law <i>and national law</i> ;	
186	(c) a secure communication infrastructure between the ESP and the EES, the VIS, [the ETIAS], Eurodac, the Central-SIS, [the ECRIS-TCN system], the Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the common identity repository (CIR) and the multiple-identity detector.	(c) a secure communication infrastructure between the ESP and the EES, the VIS, [the ETIAS], Eurodac, the Central-SIS, [the ECRIS-TCN system], the Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the common identity repository (CIR) and the multiple-identity detector.	(c) a secure communication infrastructure between the ESP and the EES, the VIS, [the ETIAS], Eurodac, the Central-SIS, [the ECRIS-TCN system], the Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the common identity repository (CIR) and the multiple-identity detector (<i>MID</i>).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
187		<i>(ca) a central Union backup ESP capable of providing all the functionalities of the principal ESP and a similar level of performance as it in the event of its failure.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
188	3. eu-LISA shall develop the ESP and ensure its technical management.	3. eu-LISA shall develop the ESP and ensure its technical management. <i>It shall not, however, have access to any of the personal data processed through the ESP.</i>	3. eu-LISA shall develop the ESP and ensure its technical management.	
189	<i>Article 7 Use of the European search portal</i>	<i>Article 7 Use of the European search portal</i>	<i>Article 7 Use of the European search portal</i>	
190	1. The use of the ESP shall be reserved to the Member State authorities and EU bodies having access to the EES, [the ETIAS], the VIS, the SIS, Eurodac and [the ECRIS-TCN system], to the CIR and the multiple-identity detector as well as the Europol data and the Interpol databases in accordance with Union or national law governing such access.	1. The use of the ESP shall be reserved to the Member State authorities and EU bodies <i>Union agencies</i> having access to the EES, [the ETIAS], the VIS, the SIS, Eurodac and [the ECRIS-TCN system] <i>in accordance with the legal instruments governing those Union information systems,</i> to the CIR and the multiple-identity detector <i>in accordance with this Regulation</i> as well as the Europol data and <i>in accordance with Regulation (EU) 2016/794 and to</i> the Interpol databases in accordance with Union or national law	1. The use of the ESP shall be reserved to the Member States authorities and EU <i>agencies</i> bodies having access <i>at least to one of the following systems or databases:</i> the EES, [the ETIAS], the VIS, the SIS, Eurodac and the [ECRIS-TCN system], to the CIR and the multiple-identity detector <i>MID</i> as well as the Europol data and the Interpol databases in accordance with Union or national law governing such access.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		governing such access. <i>Those Member State authorities and Union agencies may make use of the ESP and the data provided by it only for the objectives and purposes laid down in the legal instruments governing those Union information systems and in this Regulation.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
191	2. The authorities referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of the EES, the VIS and [the ETIAS] in accordance with their access rights under Union and national law. They shall also use the ESP to query the CIR in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.	2. The authorities referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of the EES, the VIS and [the ETIAS] in accordance with their access rights under <i>in accordance with the legal instruments governing the Union information systems</i> and national law. They shall also use the ESP to query the CIR in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.	2. The authorities referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of the EES, the VIS and [the ETIAS] in accordance with their access rights under Union and national law. They shall also use the ESP to query the CIR in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.	
192	3. The Member State authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Central SIS referred to in the [Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement]. Access to the Central SIS via the ESP shall be	3. The Member State authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Central SIS referred to in the [Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement]. Access to the Central SIS via the ESP shall be	3. The Member State authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Central SIS referred to in the [Regulation on SIS in the field of border checks <i>and Regulation on the use of SIS for the return of illegally staying third-country nationals</i> and of the Regulation	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	established through the national system (N.SIS) of each Member State in accordance with [Article 4(2) of the Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement].	established through the national system (N.SIS) of each Member State in accordance with [Article 4(2) of the Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement].	on SIS in the field of law enforcement] in accordance with their access rights under Union and national law. Access to the Central SIS via the ESP shall be established through the national system (N.SIS) of each Member State in accordance with [Article 4(2) of the Regulation on SIS in the field of border checks and of the Regulation on SIS in the field of law enforcement].	
193	4. The EU bodies shall use the ESP to search data related to persons or their travel documents in the Central SIS.	4. Where they are so required under Union law, The EU bodies Union agencies referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the Central SIS.	4. The EU agencies bodies shall use the ESP to search data related to persons or their travel documents in the Central SIS.	
194	5. The authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Interpol databases in accordance with their access rights under Union and national law.	5. Where so required under Union or national law, the authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Interpol databases in accordance with their access rights under	5. The authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Interpol databases in accordance with their access rights under Union and national law.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		Union and national law.		
195	<i>Article 8</i> <i>Profiles for the users of the European search portal</i>	<i>Article 8</i> <i>Profiles for the users of the European search portal</i>	<i>Article 8</i> <i>Profiles for the users of the European search portal</i>	
196	1. For the purposes of enabling the use of the ESP, eu-LISA shall create a profile for each category of user of the ESP in accordance with the technical details and access rights referred to in paragraph 2, including, in accordance with Union and national law:	1. For the purposes of enabling the use of the ESP, eu-LISA shall create a profile for each category of user of the ESP in accordance with the technical details and access rights referred to in paragraph 2, including, in accordance with Union and national law:	1. For the purposes of enabling the use of the ESP, eu-LISA <i>in cooperation with Member States</i> shall create a profile for each category of user of the ESP in accordance with the technical details and access rights referred to in paragraph 2, including, in accordance with Union and national law:	
197	(a) the fields of data to be used for querying;	(a) the fields of data to be used for querying;	(a) the fields of data to be used for querying;	
198		<i>(aa) the purpose of the query;</i>		
199	(b) the EU information systems, the Europol data and the Interpol databases that shall and may be consulted and that shall provide a reply to the user; and	(b) the EU <i>Union</i> information systems, the Europol data, and the Interpol databases <i>and the data in those systems</i> that shall and may be consulted <i>searched</i> and that shall provide a reply to the user; <i>a user requesting data</i>	(b) the EU information systems, the Europol data and the Interpol databases that shall and may be consulted and that shall provide a reply to the user; and	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>on the basis of Article 22 shall only get a hit/no-hit notification if the user is authorised to request from the central access point the data of the individual Union information system having provided a hit in accordance with the legal instrument governing that system; and</i>		
200	(c) the data provided in each reply.	(c) the data provided in each reply.	(c) the <i>fields of</i> data provided in each reply.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
201	2. The Commission shall adopt delegated acts in accordance with Article 63 to specify the technical details of the profiles referred to in paragraph 1 for the users of the ESP referred to in Article 7(1) in accordance with their access rights.	2. The Commission shall adopt delegated acts in accordance with Article 63 to specify the technical details of the profiles referred to in paragraph 1 for the users of the ESP referred to in Article 7(1) in accordance with their access rights <i>as laid down in the legal instruments governing Union information systems and in national law where applicable.</i>	2. The Commission shall adopt implementing delegated acts in accordance with Article 63 to specify the technical details of the profiles referred to in paragraph 1 for the users of the ESP referred to in Article 7(1) in accordance with their access rights. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
202		<i>2a. The profiles referred to in paragraph 1 shall be reviewed regularly, at least once per year, and if necessary updated.</i>		
203	Article 9 Queries	Article 9 Queries	Article 9 Queries	
204	1. The users of the ESP shall launch a query by introducing data in the ESP in accordance with their user profile and access rights. Where a query has been launched, the ESP shall query simultaneously, with the data introduced by the user of the ESP, the EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system] and the CIR as well as the Europol data and the Interpol databases.	1. The users of the ESP shall launch a query by introducing data in the ESP in accordance with their ESP user profile created in accordance with Article 8 and access rights. Where a query has been launched, the ESP shall query simultaneously, with the data introduced by the user of the ESP, the EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system] and the CIR as well as the Europol data and the Interpol databases.	1. The users of the ESP shall launch a query by introducing submitting alphanumeric and/or biometric data in to the ESP in accordance with their user profile and access rights. Where a query has been launched, the ESP shall query simultaneously, with the data submitted introduced by the user of the ESP and in accordance with the user profile and access rights , the EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system] and the CIR as well as the Europol data and the Interpol databases.	
205	2. The fields of data used to launch a query via the ESP shall correspond to the fields of data	2. The fields of data used to launch a query via the ESP shall correspond to the fields of data	2. The fields of data used to launch a query via the ESP shall correspond to the fields of data	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	related to persons or travel documents that may be used to query the various EU information systems, the Europol data and the Interpol databases in accordance with the legal instruments governing them.	related to persons or travel documents that may be used to query the various EU information systems, the Europol data and the Interpol databases in accordance with the legal instruments governing them.	related to persons or travel documents that may be used to query the various EU information systems, the Europol data and the Interpol databases in accordance with the legal instruments governing them.	
206	3. eu-LISA shall implement an interface control document (ICD) based on the UMF referred to in Article 38 for the ESP.	3. eu-LISA shall implement an interface control document (ICD) based on the UMF referred to in Article 38 for the ESP.	3. eu-LISA, <i>in cooperation with Member States</i> , shall implement an interface control document (ICD) based on the UMF referred to in Article 38 for the ESP.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
207	4. The EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system], the CIR and the multiple-identity detector, as well as the Europol data and the Interpol databases, shall provide the data that they contain resulting from the query of the ESP.	4. The EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system], the CIR and the multiple-identity detector, as well as the Europol data and the Interpol databases, shall provide the data that they contain resulting from the query of the ESP. <i>The ESP shall provide replies to the user as soon as data is available from one of the systems. The replies to the user from the ESP shall be unique and shall contain all the data to which the user has access in accordance with the legal instruments governing the Union information systems and under national law. Without prejudice to Article 20, the reply provided by the ESP shall indicate to which Union information system or database the data belongs. The ESP shall provide no information regarding data in information systems to which the user has no</i>	4. The EES, [the ETIAS], the VIS, the SIS, Eurodac, [the ECRIS-TCN system], the CIR and the multiple-identity detector, as well as the Europol data and the Interpol databases, shall provide the data that they contain resulting from the query of the ESP.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>access under Union law.</i>		
208	5. When querying the Interpol databases, the design of the ESP shall ensure that the data used by the user of the ESP to launch a query is not shared with the owners of Interpol data.	5. When querying the Interpol databases, the design of the ESP shall ensure that the data used by the user <i>no information is revealed to the owner of the Interpol alert. The design of the ESP to launch a query shall also ensure that Interpol TDAWN is not shared with the owners of Interpol data queried in a systematic manner but in accordance with applicable Union and national law.</i>	5. When querying the Interpol databases, the design of the ESP shall ensure that the data used by the user of the ESP to launch a query is not shared with the owners of Interpol data.	
209	6. The reply to the user of the ESP shall be unique and shall contain all the data to which the user has access under Union law. Where necessary, the reply provided by the ESP shall indicate to which information system or database the data belongs.	6. The reply to the user of the ESP shall be unique and shall contain all the data to which the user has access under Union law. Where necessary, the reply provided by the ESP shall indicate to which information system or database the data belongs.	6. The reply to the <i>The</i> user of the ESP shall be unique <i>receive one a reply and that</i> shall contain all <i>only</i> the data to which the user has access under Union <i>and national</i> law. Where necessary, the reply provided by the ESP shall indicate to which information system or database the data belongs.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
210	7. The Commission shall adopt a delegated act in accordance with Article 63 to specify the content and format of the ESP replies.	7. The Commission shall adopt a delegated act in accordance with Article 63 to specify the content and format of the ESP replies.	7. The Commission shall adopt an implementing delegated act in accordance with Article 63 to specify the process for querying the EU information systems, Europol data and Interpol databases by the ESP and the content and format of the ESP replies. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 64(2).	
211	<i>Article 10 Keeping of logs</i>	<i>Article 10 Keeping of logs</i>	<i>Article 10 Keeping of logs</i>	
212	1. Without prejudice to [Article 46 of the EES Regulation], Article 34 of Regulation (EC) No 767/2008, [Article 59 of the ETIAS proposal] and Articles 12 and 18 of the Regulation on SIS in the field of border checks, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:	1. Without prejudice to [Article 46 of the EES Regulation], Article 34 of Regulation (EC) No 767/2008, [Article 59 of the ETIAS proposal] and Articles 12 and 18 of the Regulation on SIS in the field of border checks, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:	1. Without prejudice to [Article 46 of the EES Regulation (EU) 2017/2226] , Article 34 of Regulation (EC) No 767/2008, [Article 69 59 of the ETIAS proposal], and Articles 12 and 18 of the Regulation on SIS in the field of border checks, eu-LISA shall keep logs of all data processing operations within the ESP. Those logs shall include, in particular, the following:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
213	(a) the Member State authority and the individual user of the ESP, including the ESP profile used as referred to in Article 8;	(a) the Member State authority and the individual user of the ESP, including the ESP profile used as referred to in Article 8 or the Union agency launching the query;	(a) the Member State authority or EU agency and the individual user of the ESP, including the ESP profile used as referred to in Article 8;	
214	(b) the date and time of the query;	(b) the date and time of the query;	(b) the date and time of the query;	
215	(c) the EU information systems and the Interpol databases queried;	(c) the EU Union information systems and the Europol and Interpol databases queried;	(c) the EU information systems and the Interpol databases queried;	
216		(ca) the ESP profile used;		
217	(d) in accordance with national rules or when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(d) in accordance with national rules or when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(d) the unique transaction identification number in accordance with national rules or when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	
218		In addition, Member States and Union agencies shall keep logs of the unique user identity of the official performing the query.		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
219			<i>1a. Each Member State shall keep logs of queries of the authority and the staff duly authorised to use the ESP including the transaction identification number referred to in point (d) of paragraph 1.</i>	
220	2. The logs may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun.	2. The logs may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, <i>for self-monitoring</i> , and for ensuring data <i>the proper functioning and data integrity</i> and security pursuant to Article 42. <i>To that end, access to those logs shall be granted as appropriate to the data controllers identified pursuant to Article 40, to national supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680, and to the European Data Protection Supervisor.</i> Those logs shall be protected by appropriate	2. The logs <i>referred to in paragraphs 1 and 1a</i> may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be <i>made available to the competent supervisory authority on request. They shall be</i> protected by appropriate measures against unauthorised access <i>and modifications</i> and erased one year after their creation, unless they are required for monitoring procedures that have already begun <i>in which case they shall be erased once the monitoring procedures no longer</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		measures against unauthorised access and erased one year two years after their creation, unless they are required for monitoring procedures that have already begun.	<i>require these logs.</i>	
221	<i>Article 11</i> <i>Fall-back procedures in case of technical impossibility to use the European search portal</i>	<i>Article 11</i> <i>Fall-back procedures in case of technical impossibility to use the European search portal</i>	<i>Article 11</i> <i>Fall-back procedures in case of technical impossibility to use the European search portal</i>	
222		-1. Where it is technically impossible to use the ESP due to its failure, eu-LISA shall switch to the back-up ESP.		
223	1. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the ESP, the users of the ESP shall be notified by eu-LISA.	1. Where it remains technically impossible to use the ESP to query one or several EU Union information systems referred to in Article 9(1) or the CIR, because of a failure of the ESP or a failure in the Union information systems being queried , the users of the ESP shall be immediately notified by eu-LISA.	1. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the ESP, the users of the ESP shall be notified automatically by eu-LISA.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
224	2. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the national infrastructure in a Member State, that Member State's competent authority shall notify eu-LISA and the Commission.	2. Where it is technically impossible to use the ESP to query one or several EU Union information systems referred to in Article 9(1) or the CIR, because of a failure of the national infrastructure in a Member State, that Member State's competent authority shall immediately inform all its users and notify eu-LISA and the Commission.	2. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the national infrastructure in a Member State, that Member State's competent authority shall notify eu-LISA and the Commission.	
225	3. In both scenarios, and until the technical failure is addressed, the obligation referred to in Article 7(2) and (4) shall not apply and Member States may access the information systems referred to in Article 9(1) or the CIR directly using their respective national uniform interfaces or national communication infrastructures.	3. In both scenarios referred to in paragraphs 1 and 2 of this Article , and until the technical failure is addressed, the obligation referred to in Article 7(2) and (4) shall not apply and Member States may shall access the Union information systems referred to in Article 9(1) or the CIR, where they are required to do so according to Union or national law , directly using their respective national uniform interfaces or national communication infrastructures.	3. In the cases referred to in paragraphs 1 or 2 both scenarios , and until the technical failure is addressed, the obligation referred to in Article 7(2) and (4) shall not apply and Member States may access the EU information systems referred to in Article 9(1) or the CIR directly using their respective national uniform interfaces or national communication infrastructures .	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
226		<i>3a. Where it is technically impossible to use the ESP to query one or several Union information systems or the CIR because of a failure of the infrastructure of a Union agency that agency shall notify eu-LISA and the Commission.</i>		
227			<i>4. Where it is technically impossible to use the ESP to query one or several EU information systems referred to in Article 9(1) or the CIR, because of a failure of the infrastructure of a EU agency, that EU agency shall notify eu-LISA and the Commission.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
228	CHAPTER III Shared Biometric Matching Service	CHAPTER III Shared Biometric Matching Service	CHAPTER III Shared Biometric Matching Service	
229	<i>Article 12 Shared biometric matching service</i>	<i>Article 12 Shared biometric matching service</i>	<i>Article 12 Shared biometric matching service</i>	
230	1. A shared biometric matching service (shared BMS) storing biometric templates and enabling querying with biometric data across several EU information systems is established for the purposes of supporting the CIR and the multiple-identity detector and the objectives of the EES, the VIS, Eurodac, the SIS and [the ECRIS-TCN system].	1. A shared biometric matching service (shared BMS) storing biometric templates and enabling querying with biometric data across several EU Union information systems containing biometric data is established for the purposes of supporting the CIR and the multiple-identity detector and the objectives of the EES, the VIS, Eurodac, the SIS and [the ECRIS-TCN system]. <i>In line with the principles of necessity and proportionality, the shared BMS shall not store DNA data or palm print data.</i>	1. A shared biometric matching service (shared BMS) storing biometric templates <i>obtained from the biometric data referred to in Article 13, that are stored in the CIR and the SIS,</i> and enabling querying with biometric data across several EU information systems is established for the purposes of supporting the <i>Common Identity Repository (CIR)</i> and the multiple-identity detector (<i>MID</i>) and the objectives of the EES, the VIS, Eurodac, the SIS and [the ECRIS-TCN system].	
231	2. The shared BMS shall be composed of:	2. The shared BMS shall be composed of:	2. The shared BMS shall be composed of:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
232	(a) a central infrastructure, including a search engine and the storage of the data referred to in Article 13;	(a) a central infrastructure, including a <i>that shall replace the Automated Fingerprint Identification Systems of respectively the EES, VIS, SIS, Eurodac and [ECRIS-TCN] to the extent that it allows to</i> search engine and the storage of the data referred with biometric data as defined in Article 13 <i>4(12)</i> ;	(a) a central infrastructure, including a search engine and the storage of the data referred to in Article 13;	
233	(b) a secure communication infrastructure between the shared BMS, Central-SIS and the CIR.	(b) a secure communication infrastructure between the shared BMS, Central-SIS, and <i>the Union information systems.</i>	(b) a secure communication infrastructure between the shared BMS, Central-SIS and the CIR.	
234	3. eu-LISA shall develop the shared BMS and ensure its technical management.	3. eu-LISA shall develop the shared BMS and ensure its technical management. <i>It shall not, however, have access to any of the personal data processed through the shared BMS.</i>	3. eu-LISA shall develop the shared BMS and ensure its technical management.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
235	<i>Article 13</i> <i>Data stored in the shared biometric matching service</i>	<i>Article 13</i> Data stored Storing biometric templates in the shared biometric matching service	<i>Article 13</i> <i>Data stored in the shared biometric matching service</i>	
236	1. The shared BMS shall store the biometric templates that it shall obtain from the following biometric data:	1. The shared BMS shall store the biometric templates – logically separated – according to the information system from which the data originates , that it shall obtain from the following biometric data:	1. The shared BMS shall store the biometric templates that it shall obtain from the following biometric data:	
237	(a) the data referred to in Article 16(1)(d) and Article 17(1)(b) and (c) of Regulation (EU) 2017/2226;	(a) the data referred to in Article 16(1)(d) and Article 17(1)(b) and (c) of Regulation (EU) 2017/2226;	(a) the data referred to in Article 16(1)(d) and Article 17(1)(b) and (c) and Article 18(2)(a), (b) and (c) of Regulation (EU) 2017/2226;	
238	(b) the data referred to in Article 9(6) of Regulation (EC) No 767/2008;	(b) the data referred to in Article 9(6) of Regulation (EC) No 767/2008;	(b) the data referred to in Article 9(5) and (6) of Regulation (EC) No 767/2008;	
239	(c) [the data referred to in Article 20(2)(w) and (x) of the Regulation on SIS in the field of border checks;	(c) [the data referred to in Article 20(2)(w) and (x) of the Regulation on SIS in the field of border checks;	(c) [the data referred to in Article 20(2)(w) and (x) of the Regulation on SIS in the field of border checks;	
240	(d) the data referred to in	(d) the data referred to in	(d) the data referred to in	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Article 20(3)(w) and (x) of the Regulation on SIS in the field of law enforcement;	Article 20(3)(w) and (x) (y) of the Regulation on SIS in the field of law enforcement;	Article 20(3)(w) and (x) of the Regulation on SIS in the field of law enforcement;	
241	(e) the data referred to in Article 4(3)(t) and (u) of the Regulation on SIS in the field of illegal return];	(e) the data referred to in Article 4(3)(t) and (u) of the Regulation on SIS in the field of illegal return];	(e) [the data referred to in Article 4(t) and (u) of the Regulation on SIS <i>for the return of illegally staying third-country nationals</i> in the field of illegal return];	
242	(f) [the data referred to in Article 13(a) of the Eurodac Regulation;]	(f) [the data referred to in Article 13(a) 12(a) and (b), Article 13(2),(a) and (b) and Article 14(2),(a) and (b) of the Eurodac Regulation;]	(f) — [the data referred to in Article 13(a) of the Eurodac Regulation;]	
243	(g) [the data referred to in Article 5(1)(b) and Article 5(2) of the ECRIS-TCN Regulation.]	(g) [the data referred to in Article 5(1)(b) and Article 5(2) of the ECRIS-TCN Regulation.]	(g) — [the data referred to in Article 5(1)(b) and Article 5(2) of the ECRIS-TCN Regulation.]	
244			<i>The shared BMS shall store the biometric templates - logically separated - according to the EU information system from which the data originated.</i>	
245	2. The shared BMS shall include in each biometric template a reference to the information systems in which the	2. The shared BMS shall include in each biometric template a reference to the information systems in which the	2. <i>For each set of data referred to in paragraph 1, the shared BMS shall include in each biometric template a reference to</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	corresponding biometric data is stored.	corresponding biometric data is stored.	the <i>EU</i> information systems <i>and a reference to the actual record in the EU information systems</i> in which the corresponding biometric data <i>are</i> is-stored.	
246	3. Biometric templates shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the information systems performed by the shared BMS to ascertain the fulfilment of a minimum data quality standard.	3. Biometric templates shall only be entered in the shared BMS following an automated quality check of the biometric data added to one of the information systems performed by the shared BMS to ascertain the fulfilment of a minimum data quality standard.	3. Biometric templates shall only <i>may</i> be entered <i>only</i> in the shared BMS following an automated quality check of the biometric data added to one of the <i>EU</i> information systems performed by the shared BMS to ascertain the fulfilment of a minimum data quality standard.	
247	4. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).	4. The storage of the data referred to in paragraph 1 <i>of this Article</i> shall meet the quality standards referred to in Article 37(2) <i>37</i> .	4. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2) <i>and (4)</i> .	
248			5. <i>The Commission shall lay down the performance requirements and performance monitoring of the shared BMS, including the minimum requirements regarding the biometric performance of the</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>shared BMS, in particular in terms of the required False Positive Identification Rate, False Negative Identification Rate and Failure To Enrol Rate, as well as the procedures and tools for notifying False Positive Identifications and False Negative verifications to eu-LISA in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).</i>	
249			<i>For the specific purpose of monitoring the performance of the shared BMS, Member States shall be allowed to use the biometric templates stored in the shared BMS.</i>	
250	<i>Article 14 Searching biometric data with the shared biometric matching service</i>	<i>Article 14 Searching biometric data with the shared biometric matching service</i>	<i>Article 14 Searching biometric data with the shared biometric matching service</i>	
251	In order to search the biometric data stored within the CIR and	In order to search the biometric data stored within the CIR and	In order to search the biometric data stored within the CIR and	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	the SIS, the CIR and the SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in the EES Regulation, the VIS Regulation, the Eurodac Regulation, the [SIS Regulations] and [the ECRIS-TCN Regulation].	the SIS, the CIR and the SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in the EES Regulation, the VIS Regulation, the Eurodac Regulation, the [SIS Regulations] and [the ECRIS-TCN Regulation].	the SIS, the CIR and the SIS shall use the biometric templates stored in the shared BMS. Queries with biometric data shall take place in accordance with the purposes provided for in this Regulation and in the EES Regulation (EU) 2017/2226, the VIS Regulation (EC) No 767/2008, the Eurodac Regulation, the [SIS Regulations] and [the ECRIS-TCN Regulation].	
252	<i>Article 15</i> <i>Data retention in the shared biometric matching service</i>	<i>Article 15</i> <i>Data retention in the shared biometric matching service</i>	<i>Article 15</i> <i>Data retention in the shared biometric matching service</i>	
253	The data referred to in Article 13 shall be stored in the shared BMS for as long as the corresponding biometric data is stored in the CIR or the SIS.	The data referred to in Article 13 shall be stored in the shared BMS for as long as the corresponding biometric data is stored in the CIR <i>in accordance with Articles 18 and 19</i> or the SIS <i>or in SIS, after which it shall be automatically deleted.</i>	The data referred to in Article 13(1) <i>and</i> (2) shall be stored in the shared BMS for as long as the corresponding biometric data <i>are</i> is stored in the CIR or the SIS <i>and shall be erased in an automated manner.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
254	<i>Article 16 Keeping of logs</i>	<i>Article 16 Keeping of logs</i>	<i>Article 16 Keeping of logs</i>	
255	1. Without prejudice to [Article 46 of the EES Regulation], Article 34 of Regulation (EC) No 767/2008 and [Article 12 and 18 of the Regulation on SIS in the field of law enforcement], eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include, in particular, the following:	1. Without prejudice to [Article 46 of the EES Regulation], Article 34 of Regulation (EC) No 767/2008 and [Article 12 and 18 of the Regulation on SIS in the field of law enforcement border checks], eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include, in particular, the following:	1. Without prejudice to [Article 46 of the EES Regulation] (EU) 2017/2226 , Article 34 of Regulation (EC) No 767/2008, and [Article 12 and 18 of the Regulation on SIS in the field of law enforcement border checks], eu-LISA shall keep logs of all data processing operations within the shared BMS. Those logs shall include, in particular, the following:	
256		(-a) the Member State authority or the Union agency launching the query;		
257	(a) the history related to the creation and storage of biometric templates;	(a) the history related to the creation and storage of biometric templates;	(a) the history related to the creation and storage of biometric templates;	
258	(b) a reference to the EU information systems queried with the biometric templates stored in the shared BMS;	(b) a reference to the EU information systems queried with the biometric templates stored in the shared BMS;	(b) a reference to the EU information systems queried with the biometric templates stored in the shared BMS;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
259	(c) the date and time of the query;	(c) the date and time of the query;	(c) the date and time of the query;	
260	(d) the type of biometric data used to launch the query;	(d) the type of biometric data used to launch the query;	(d) the type of biometric data used to launch the query;	
261	(e) the length of the query;	(e) the length of the query;	(e) the length of the query;	
262	(f) the results of the query and date and time of the result;	(f) the results of the query and <i>the</i> date and time of the result <i>and the Union information system from which the data was received</i> ;	(f) the results of the query and date and time of the result;	
263	(g) in accordance with national rules or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(g) in accordance with national rules or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(g) in accordance with national rules or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query <i>the Member State or EU agency searching biometric data.</i>	
264		<i>(ga) the specific purpose of the query and, where applicable, the case reference, pursuant to Article 14.</i>		
265		<i>In addition, Member States and Union agencies shall keep logs of the unique user identity of the</i>	<i>1a. Each Member State shall keep logs of queries of the authority and the staff duly</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>official performing the query.</i>	<i>authorised to use the shared BMS.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
266	<p>2. The logs may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun. The logs referred to in paragraph 1(a) shall be erased once the data is erased.</p>	<p>2. The logs may be used only for data protection monitoring <i>and monitoring the impact on fundamental rights</i>, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. <i>To that end, access to those logs shall be granted as appropriate to the data controllers identified pursuant to Article 40, to the national supervisory authorities referred to in Article 51 of Regulation (EU) 2016/679 and Article 41 of Directive (EU) 2016/680, and to the European Data Protection Supervisor.</i> Those logs shall be protected by appropriate measures against unauthorised access and erased one year <i>two years</i> after their creation, unless they are required for monitoring procedures that have already begun. The logs referred to in paragraph 1(a) shall</p>	<p>2. The logs <i>referred to in paragraphs 1 and 1a</i> may be used only for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be <i>made available to the competent supervisory authority on request. They shall</i> protected by appropriate measures against unauthorised access <i>and modifications</i> and erased one year after their creation, unless they are required for monitoring procedures that have already begun, <i>in which case they shall be erased once the monitoring procedures no longer require these logs.</i> The logs referred to in paragraph 1(a) shall be erased once the data is <i>are</i> is-erased.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		be erased once the data is erased.		
267	CHAPTER IV Common Identity Repository	CHAPTER IV Common Identity Repository	CHAPTER IV Common Identity Repository	
268	<i>Article 17 Common identity repository</i>	<i>Article 17 Common identity repository</i>	<i>Article 17 Common identity repository</i>	
269	1. A common identity repository (CIR), creating an individual file for each person that is recorded in the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system] containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system], of supporting the functioning of the multiple-identity detector and of facilitating and streamlining access by law enforcement authorities to non-law	1. A common identity repository (CIR), creating an individual file for each person that is recorded in the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system] containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system], of supporting the functioning of the multiple-identity detector and of facilitating and streamlining access by law enforcement <i>designated</i> authorities to non-law	1. A common identity repository (CIR), creating an individual file for each person that is recorded in the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system] containing the data referred to in Article 18, is established for the purpose of facilitating and assisting the correct identification of persons registered in the EES, the VIS, [the ETIAS], the Eurodac and [the ECRIS-TCN system] <i>in accordance with Article 20</i> , of supporting the functioning of the multiple-identity detector <i>in accordance with Article 21</i> and of facilitating and streamlining access by law	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	enforcement information systems at EU level, where necessary for the prevention, investigation, detection or prosecution of serious crime.	enforcement information systems at EU Union level, where necessary for the prevention, investigation, detection or prosecution of serious crime, while fully respecting the principles of necessity and proportionality.	enforcement designated authorities and Europol to non-law enforcement EU information systems at EU level , where necessary for the prevention, investigation , detection or investigation or prosecution of terrorist offences or other of serious crime criminal offences in accordance with Article 22.	
270	2. The CIR shall be composed of:	2. The CIR shall be composed of:	2. The CIR shall be composed of:	
271	(a) a central infrastructure that shall replace the central systems of respectively the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system] to the extent that it shall store the data referred to in Article 18;	(a) a central infrastructure that shall replace the central systems of respectively the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system] to the extent that it shall store the data referred to in Article 18;	(a) a central infrastructure that shall replace the central systems of respectively the EES, the VIS, [the ETIAS], Eurodac and [the ECRIS-TCN system] to the extent that it shall store the data referred to in Article 18;	
272	(b) a secure communication channel between the CIR, Member States and EU bodies that are entitled to use the European search portal (ESP) in accordance with Union law;	(b) a secure communication channel between the CIR, Member States and EU bodies Union agencies that are entitled to use the European search portal (ESP) CIR in accordance with Union and national law	(b) a secure communication channel between the CIR, Member States and EU bodies agencies that are entitled to use the European search portal (ESP) CIR in accordance with Union law and national law ;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
273	(c) a secure communication infrastructure between the CIR and the EES, [the ETIAS], the VIS, Eurodac and [the ECRIS-TCN system] as well as with the central infrastructures of the ESP, the shared BMS and the multiple-identity detector.	(c) a secure communication infrastructure between the CIR and the EES, [the ETIAS], the VIS, Eurodac and [the ECRIS-TCN system] as well as with the central infrastructures of the ESP, the shared BMS and the multiple-identity detector.	(c) a secure communication infrastructure between the CIR and the EES, [the ETIAS], the VIS, Eurodac and [the ECRIS-TCN system] as well as with the central infrastructures of the ESP, the shared BMS and the <i>MID</i> multiple-identity detector .	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
274		<i>(ca) a central Union backup CIR capable of providing all the functionalities of the principal CIR and a similar level of performance as it in the event of its failure. The CIR and the backup CIR may operate simultaneously. The CIR and the backup CIR shall be located in technical sites of eu-LISA.</i>		
275	3. eu-LISA shall develop the CIR and ensure its technical management.	3. eu-LISA shall develop the CIR and ensure its technical management.	3. eu-LISA shall develop the CIR and ensure its technical management.	
276		<i>3a. Where it is technically impossible to query the CIR for the purpose of identifying a person pursuant Article 20, for the detection of multiple identities pursuant Article 21 or for law enforcement purposes pursuant Article 22, because of a failure of the CIR, the users of the CIR shall be immediately notified by eu-LISA.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
277			4. eu-LISA, in cooperation with Member States, shall implement an interface control document based on the UMF referred to in Article 38 for the CIR.	
278	<i>Article 18 The common identity repository data</i>	<i>Article 18 The common identity repository data</i>	<i>Article 18 The common identity repository data</i>	
279	1. The CIR shall store the following data – logically separated – according to the information system from which the data was originated:	1. The CIR shall store the following data – logically separated – according to the information system from which the data was originated:	1. The CIR shall store the following data – logically separated – according to the EU information system from which the data was originated:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
280	(a) the data referred to in [Article 16(1)(a) to (d) and Article 17(1)(a) to (c) of the EES Regulation];	(a) the data referred to in [Article 16(1)(a) to (d) and Article 17(1)(a) to (c) of the EES Regulation];	(a) the data referred to in {Article 16(1)(a) to (d), and Article 17(1)(a) to (c) and Article 18(1) and (2) of the EES Regulation (EU) 2017/2226};	
281	(b) the data referred to in Article 9(4)(a) to (c), (5) and (6) of Regulation (EC) No 767/2008;	(b) the data referred to in Article 9(4)(a) to (c), (5) and (6) of Regulation (EC) No 767/2008;	(b) the data referred to in Article 9(4)(a) to (c), (5) and (6) of Regulation (EC) No 767/2008;	
282	(c) [the data referred to in Article 15(2)(a) to (e) of the [ETIAS Regulation;]	(c) [the data referred to in Article 15(2)(a) to (e) of the [ETIAS Regulation;]	(c) [the data referred to in Article 17(2) (a), (b), (c), (d) and (e) 15(2)(a) to (e) of the [ETIAS Regulation;]	
283	(d) – (not applicable)	(d) — (not applicable) (Horizontal amendment applies throughout the text.)	(d) — (not applicable)	
284	(e) – (not applicable)	(e) — (not applicable)	(e) — (not applicable)	
285	2. For each set of data referred to in paragraph 1, the CIR shall include a reference to the information systems to which the data belongs.	2. For each set of data referred to in paragraph 1, the CIR shall include a reference to the information systems to which the data belongs. The officer accessing the CIR shall see only the data contained in the individual file stored in the CIR	2. For each set of data referred to in paragraph 1, the CIR shall include a reference to the EU information systems to which the data belongs.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>which originate from those information systems the officer is authorised to access.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
286			<i>2a. For each set of data referred to in paragraph 1, the CIR shall include a reference to the actual record in the EU information systems to which the data belongs.</i>	
287	3. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).	3. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2).	3. The storage of the data referred to in paragraph 1 shall meet the quality standards referred to in Article 37(2) and (4) .	
288	<i>Article 19 Adding, amending and deleting data in the common identity repository</i>	<i>Article 19 Adding, amending and deleting data in the common identity repository</i>	<i>Article 19 Adding, amending and deleting data in the common identity repository</i>	
289	1. Where data is added, amended or deleted in the EES, the VIS and [the ETIAS], the data referred to in Article 18 stored in the individual file of the CIR shall be added, amended or deleted accordingly in an automated manner.	1. Without duplicating the data from the respective Union information systems , where data is added, amended or deleted in the EES, the VIS and [the ETIAS], the data referred to in Article 18 stored in the individual file of the CIR shall be simultaneously added, amended or deleted accordingly in an	1. Where data is are added, amended or deleted in the EES, the VIS and [the ETIAS], the data referred to in Article 18 stored in the individual file of the CIR shall be added, amended or deleted accordingly in an automated manner.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		automated manner.		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
290	2. Where the multiple-identity detector creates a white or red link in accordance with Articles 32 and 33 between the data of two or more of the EU information systems constituting the CIR, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data.	2. Where the multiple-identity detector creates a white or red link in accordance with Articles 32 and 33 between the data of two or more of the EU information systems constituting the CIR, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data.	2. Where the multiple-identity detector creates a white or red link <i>is created in the MID</i> in accordance with Articles 32 and or 33 between the data of two or more of the EU information systems constituting the CIR, instead of creating a new individual file, the CIR shall add the new data to the individual file of the linked data.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
291	Article 20 Access to the common identity repository for identification	Article 20 Access to the common identity repository for identification	Article 20 Access to the common identity repository for identification	
292		-1 Where a Member State police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity, or where there are doubts about the identity data provided by that person or as to the authenticity of the travel document or the identity of its holder or where the person is unable or refuses to cooperate, the authority shall be able to query the CIR in accordance with paragraphs 1 and 2. Such query shall not be allowed against minors under the age of 12 years old, unless in the best interest of the child.		
293	1. Where a Member State police authority has been so empowered by national legislative measures as referred to	Where <i>the situation referred to in paragraph -1 arises during an identity check following rules and procedures provided for in</i>	1. Where a Member State police authority has been so empowered by national legislative measures as referred to	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>in paragraph 2, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken during an identity check.</p>	<p><i>national law and</i> a Member State police authority has been so empowered by national legislative measures as referred to in paragraph 2, it may, <i>in the presence of that person, and</i> solely for the purpose of identifying <i>that</i> person, query the CIR with the biometric data of that person taken during an <i>the</i> identity check.</p>	<p>in paragraph 2, it may, solely for the purpose of identifying a person, query the CIR with the biometric data of that person taken during an identity check.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
294			1a. <i>Where a police authority has been so empowered by national legislative measures as referred to in paragraph 2a, it may, for the purpose of identifying unknown persons who are not able to identify themselves or unidentified human remains, in the event of a disaster or an accident, query the CIR with the biometric data of those persons.</i>	
295	Where the query indicates that data on that person is stored in the CIR, the Member States authority shall have access to consult the data referred to in Article 18(1).	Where the query indicates that data on that person is stored in the CIR, the Member States <i>police</i> authority shall have access to consult the data referred to in Article 18(1). <i>The consultation shall not reveal to which Union information system the data belongs.</i>	1b. Where the query indicates that data on that person is stored in the CIR, the Member States <i>police</i> authority shall have access to consult the data referred to in Article 18(1).	
296	Where the biometric data of the person cannot be used or where the query with that data fails, the query shall be carried out with identity data of the person in combination with travel	Where the biometric data of the person cannot be used or where the query with that data fails, the query shall be carried out with identity data of the person in combination with travel	Where the biometric data of the person cannot be used or where the query with that data fails, the query shall be carried out with identity data of the person in combination with travel	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	document data, or with the identity data provided by that person.	document data, or with the identity data provided by that person.	document data, or with the identity data provided by that person.	
297		<i>1a. Where a Member State police authority has been so empowered by national legislative measures as referred to in paragraph 2, it may, in the event of a disaster or an accident and solely for the purpose of identifying unknown persons who are not able to identify themselves or unidentified human remains, query the CIR with the biometric data of those persons.</i>		
298	2. Member States wishing to avail themselves of the possibility provided for in this Article shall adopt national legislative measures. Such legislative measures shall specify the precise purposes of identity checks within the purposes referred to in Article 2(1)(b) and (c). They shall designate the police authorities competent and lay down the	2. Member States wishing to avail themselves of the possibility provided for in this Article shall adopt national legislative measures. Such legislative measures shall specify the precise purposes of identity checks the identification within the purposes referred to in Article 2(2)(b) 2(1)(b) and (c). They shall designate the police authorities	2. Member States wishing to avail themselves of the possibility provided for in paragraph 1 this Article shall adopt national legislative measures. Such legislative measures shall specify the precise purposes of identity checks within the purposes referred to in Article 2(1)(b) and (c). They shall designate the police authorities competent and	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>procedures, conditions and criteria of such checks.</p>	<p>competent and lay down the procedures, conditions and criteria of such checks <i>for such identification. They shall designate the competent police authorities. Member States making use of this possibility shall transmit the text of their national legislative measures to the Commission. Access to the CIR to establish the identity of a third country national for purposes of ensuring a high level of security shall only be allowed where access for the same purposes to similar national databases exist and under equivalent conditions.</i></p>	<p>lay down the procedures, conditions and criteria of such checks.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
299			<i>2a. Member States wishing to avail themselves of the possibility provided for in paragraph 1a shall adopt national legislative measures laying down the procedures, conditions and criteria.</i>	
300	<i>Article 21 Access to the common identity repository for the detection of multiple identities</i>	<i>Article 21 Access to the common identity repository for the detection of multiple identities</i>	<i>Article 21 Access to the common identity repository for the detection of multiple identities</i>	
301	1. Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the verification of different identities determined in accordance with Article 29 shall have access, solely for the purpose of that verification, to the identity data stored in the CIR belonging to the various information systems connected to a yellow link.	1. Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the verification of different identities determined in accordance with Article 29 shall have access, solely for the purpose of that verification, to the identity data stored in the CIR belonging to the various information systems connected to a yellow link.	1. Where a query of the CIR results in a yellow link in accordance with Article 28(4), the authority responsible for the verification of different identities determined in accordance with Article 29 shall have access, solely for the purpose of that verification, to the identity data referred to in Article 18(1) and (2) stored in the CIR belonging to the various EU information systems connected to a yellow link.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
302	2. Where a query of the CIR results in a red link in accordance with Article 32, the authorities referred to in Article 26(2) shall have access, solely for the purposes of fighting identity fraud, to the identity data stored in the CIR belonging to the various information systems connected to a red link.	2. Where a query of the CIR results in a red link in accordance with Article 32, the authorities referred to in Article 26(2) shall have access, solely for the purposes of fighting identity fraud, to the identity data stored in the CIR belonging to the various information systems connected to a red link.	2. Where a query of the CIR results in a red link in accordance with Article 32, the authorities referred to in Article 26(2) shall have access, solely for the purposes of fighting identity fraud, to the identity data referred to in Article 18(1) and (2) stored in the CIR belonging to the various EU information systems connected to a red link.	
303	<i>Article 22</i> <i>Querying the common identity repository for law enforcement purposes</i>	<i>Article 22</i> <i>Querying the common identity repository for law enforcement purposes</i>	<i>Article 22</i> <i>Querying the common identity repository for law enforcement purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences</i>	
304	1. For the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case and in order to obtain information on whether data on a specific person is present in the EES, the VIS and	1. For the purposes of preventing, detecting and investigating Where there are reasonable grounds to believe that consultation of Union information systems will substantially contribute to the prevention, detection or	1. For the purposes of preventing, detecting and or investigating terrorist offences or other serious criminal offences in a specific case and in order to obtain information on whether data on a specific person is present in the EES, the VIS and	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	[the ETIAS] or the Member State designated authorities and Europol may consult the CIR.	<i>investigation of</i> terrorist offences or other serious criminal offences in a specific case and , <i>in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category of third-country nationals whose data are stored in [the EES], VIS, [ETIAS], and where a prior search in national databases has been carried out and a query of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA has been launched, the Member States designated authorities and Europol may use the CIR</i> in order to obtain information on whether data on a specific person is present in the EES, the VIS and the [ETIAS] or the Member State designated authorities and Europol may consult the CIR.	[the ETIAS] or the Member State designated authorities and Europol may consult the CIR.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
305	2. Member State designated authorities and Europol shall not be entitled to consult data belonging to [the ECRIS-TCN] when consulting the CIR for the purposes listed in paragraph 1.	2. Member State designated authorities and Europol shall not be entitled to consult data belonging to [the ECRIS-TCN] when consulting the CIR for the purposes listed in paragraph 1.	2. Member State designated authorities and Europol shall not be entitled to consult data belonging to [the ECRIS-TCN] when consulting the CIR for the purposes listed in paragraph 1.	
306	3. Where, in reply to a query the CIR indicates data on that person is present in the EES, the VIS and [the ETIAS] the CIR shall provide to Member States' designated authorities and Europol a reply in the form of a reference indicating which of the information systems contains matching data referred to in Article 18(2). The CIR shall reply in such a way that the security of the data is not compromised.	3. Where, in reply to a query the CIR indicates data on that person is present in the EES, the VIS and [the ETIAS] the CIR shall provide to Member States' designated authorities and Europol a reply in the form of a reference indicating which of the information systems contains matching data referred to in Article 18(2). The CIR shall reply in such a way that the security of the data is not compromised.	3. Where, in reply to a query, the CIR indicates data on that person is present in the EES, the VIS and [the ETIAS], the CIR shall provide to Member States' designated authorities and Europol a reply in the form of a reference indicating which of the <i>EU</i> information systems contains matching data referred to in Article 18(2). The CIR shall reply in such a way that the security of the data is not compromised. <i>The reply indicating that data on that person is present in any of those systems may be used only for the purpose of submitting an access request subject to the conditions and procedures laid down in the respective legislative instruments governing such access.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
307		<i>The reply indicating that data on that person is present in any of the Union information systems referred to in paragraph 1 may be used only for the purposes of submitting an access request subject to the conditions and procedures laid down in the respective legislative instruments governing such access.</i>		
308	4. Full access to the data contained in the EU information systems for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences remains subject to the conditions and procedures laid down in the respective legislative instruments governing such access.	4. Full access to the data contained in the EU information systems for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences remains subject to the conditions and procedures laid down in the respective legislative instruments governing such access.	4. Full access to the data contained in the EU information systems for the purposes of preventing, detecting and <i>or</i> investigating terrorist offences or other serious criminal offences remains subject to the conditions and procedures laid down in the respective legislative instruments governing such access.	
309		<i>4a. The Member State designated authorities and Europol getting a hit shall refer to the national supervisory authorities that shall check whether the conditions of accessing the CIR were complied</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>with. In case the ex post independent verification determines that the consultation of the CIR was not justified, the law enforcement authority shall erase all data originating from the CIR.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
310	Article 23 Data retention in the common identity repository	Article 23 Data retention in the common identity repository	Article 23 Data retention in the common identity repository	
311	1. The data referred to in Article 18(1) and (2) shall be deleted from the CIR in accordance with the data retention provisions of [the EES Regulation], the VIS Regulation and [the ETIAS Regulation] respectively.	1. The data referred to in Article 18(1) and (2) shall be automatically deleted from the CIR in accordance with the data retention provisions of [the EES Regulation], the VIS Regulation and [the ETIAS Regulation] respectively.	1. Without prejudice to paragraphs 2 and 3, the data referred to in Article 18(1), and (2) and (2a) shall be deleted from the CIR in an automated manner in accordance with the data retention provisions of the EES Regulation (EU) 2017/2226 , the VIS Regulation (EC) No 767/2008 and [the ETIAS Regulation] respectively.	
312	2. The individual file shall be stored in the CIR for as long as the corresponding data is stored in at least one of the information systems whose data is contained in the CIR. The creation of a link shall not affect the retention period of each item of the linked data.	2. The individual file shall be stored in the CIR for as long as the corresponding data is stored in at least one of the Union information systems whose data is contained in the CIR. The creation of a link shall not affect the retention period of each item of the linked data. Once all data to which a link is created is deleted the link shall also be deleted automatically.	2. The individual file shall be stored in the CIR for as long as the corresponding data are is stored in at least one of the EU information systems whose data are is contained in the CIR. The creation of a link shall not affect the retention period of each item of the linked data.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
313			3. Where a red link is stored in the MID in accordance with Article 32, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR for as long as the corresponding data are stored in at least one of the EU information systems from which the linked data originates.	
314	<i>Article 24 Keeping of logs</i>	<i>Article 24 Keeping of logs</i>	<i>Article 24 Keeping of logs</i>	
315	1. Without prejudice to [Article 46 of the EES Regulation], Article 34 of Regulation (EC) No 767/2008 and [Article 59 of the ETIAS proposal], eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4.	1. Without prejudice to [Article 46 of the EES Regulation], Article 34 of Regulation (EC) No 767/2008 and [Article 59 of the ETIAS proposal], eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4.	1. Without prejudice to [Article 46 of the EES Regulation (EU) 2017/2226 , Article 34 of Regulation (EC) No 767/2008 and [Article 69 59 of the ETIAS proposal], eu-LISA shall keep logs of all data processing operations within the CIR in accordance with paragraphs 2, 3 and 4.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
316	2. Concerning any access to the CIR pursuant to Article 20, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	2. Concerning any access to the CIR pursuant to Article 20, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	2. Concerning any access to the CIR pursuant to Article 20, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
317		<i>(-a) the Member State authority launching the query;</i>		
318	(a) the purpose of access of the user querying via the CIR;	(a) the purpose of access of the user querying via the CIR;	(a) the purpose of access of the user querying via the CIR;	
319	(b) the date and time of the query;	(b) the date and time of the query;	(b) the date and time of the query;	
320	(c) the type of data used to launch the query;	(c) the type of data used to launch the query;	(c) the type of data used to launch the query;	
321	(d) the results of the query;	(d) the results of the query <i>and the Union information system from which the data was received.;</i>	(d) the results of the query;	
322	(e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query <i>the Member State or EU agency querying the CIR.</i>	
323		<i>In addition, Member States shall keep logs of the unique user identity of the official performing the query.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
324	3. Concerning any access to the CIR pursuant to Article 21, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	3. Concerning any access to the CIR pursuant to Article 21, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	3. Concerning any access to the CIR pursuant to Article 21, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
325		<i>(-a) the Member State authority launching the query;</i>		
326	(a) the purpose of access of the user querying via the CIR;	(a) the purpose of access of the user querying via the CIR;	(a) the purpose of access of the user querying via the CIR;	
327	(b) the date and time of the query;	(b) the date and time of the query;	(b) the date and time of the query;	
328	(c) where relevant, the data used to launch the query;	(c) where relevant, the data used to launch the query;	(c) where relevant <i>a link is created</i> , the data used to launch the query;	
329	(d) where relevant, the results of the query;	(d) where relevant, the results of the query <i>and the Union information system from which the data was received.</i>	(d) where relevant <i>a link is created</i> , the results of the query;	
330	(e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query.	(e) in accordance with national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the person who carried out the query <i>the Member State or EU agency querying the CIR.</i>	
331		<i>In addition, Member States shall keep logs of the unique user identity of the official</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>performing the query.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
332	4. Concerning any access to the CIR pursuant to Article 22, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	4. Concerning any access to the CIR pursuant to Article 22, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	4. Concerning any access to the CIR pursuant to Article 22, eu-LISA shall keep logs of all data processing operations within the CIR. Those logs shall include, in particular, the following:	
333	(a) the national file reference;	(a) <i>the purpose of access and the reference to the national file reference investigation or case;</i>	(a) the national file reference;	
334	(b) the date and time of the query;	(b) the date and time of the query;	(b) the date and time of the query;	
335	(c) the type of data used to launch the query;	(c) <i>the data used to launch the query or, in the case of a query launched with biometric data,</i> the type of data used to launch the query;	(c) the type of data used to launch the query;	
336	(d) the results of the query;	(d) the results of the query <i>and the Union information system from which the data was received.;</i>	(d) the results of the query;	
337	(e) the name of the authority consulting the CIR;	(e) the name of the authority consulting the CIR;	(e) the name of the authority consulting the CIR; <i>Member State or EU agency querying</i>	
338	(f) in accordance with national rules or with Regulation	(f) in accordance with	(f) <i>when applicable,</i> in accordance with national rules or	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	(EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the official who carried out the query and of the official who ordered the query.	national rules or with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark of the official who carried out the query and of the official who ordered the query.	with Regulation (EU) 2016/794 or, when applicable, Regulation (EU) 45/2001, the identifying mark <i>unique user identity</i> of the official who carried out the query and of the official who ordered the query <i>in accordance with Regulation (EU) 2016/794 or [Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC].</i>	
339		<i>In addition, Member States shall keep logs of the unique user identity of the official performing the query.</i>		
340	The logs of such access shall be regularly verified by the competent supervisory authority established in accordance with	The logs of such access shall be regularly verified by the competent supervisory authority established in accordance with	The logs of such access shall be regularly verified by the competent supervisory authority established in accordance with	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Article 51 of Regulation (EU) 2016/679 or in accordance with Article 41 of Directive 2016/680, at intervals not exceeding six months, to verify whether the procedures and conditions set out in Article 22(1) to (3) are fulfilled.	Article 51 of Regulation (EU) 2016/679 or in accordance with Article 41 of Directive 2016/680, at intervals not exceeding six months, to verify whether the procedures and conditions set out in Article 22(1) to (3) are fulfilled. <i>eu-LISA shall make available to the supervisory authorities a practical tool to facilitate and automate as far as possible the verification of the logs.</i>	Article 51 of Regulation (EU) 2016/679, or in accordance with Article 41 of Directive 2016/680 <i>or by the European Data Protection Supervisor in accordance with Article 43 of Regulation (EU) 2016/794</i> , at intervals not exceeding six months <i>one year</i> , to verify whether the procedures and conditions set out in Article 22(1) to (3) are fulfilled.	
341	5. Each Member State shall keep logs of queries of the staff duly authorised to use the CIR pursuant to Articles 20, 21 and 22.	5. Each Member State shall keep logs of queries of the staff duly authorised to use the CIR pursuant to Articles 20, 21 and 22.	5. Each Member State shall keep logs of queries of <i>the authority and</i> the staff duly authorised to use the CIR pursuant to Articles 20, 21 and 22.	
342			<i>In addition, for any access to the CIR pursuant to Article 22, each Member State shall keep the following logs:</i>	
343			<i>(a) the national file reference;</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
344			<i>(b) in accordance with national rules, the unique user identity of the official who carried out the query and of the official who ordered the query.</i>	
345		<i>5a. Union agencies shall keep logs of queries of the staff duly authorised to use the CIR pursuant to Article 22.</i>		
346			<i>5a. Europol shall keep logs of queries of the staff duly authorised to use the CIR pursuant to Article 22.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
347	6. The logs referred to in paragraphs 1 and 5 may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. They shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun.	6. The logs referred to in paragraphs 1 and 5 , 5 and 5a may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, for self-monitoring , and for ensuring the proper functioning and the data integrity and data security pursuant to Article 42. They shall be protected by appropriate measures against unauthorised access and erased two years one year after their creation, unless they are required for monitoring procedures that have already begun.	6. The logs referred to in paragraphs 1, 5 and 5a may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. They shall be protected by appropriate measures against unauthorised access and modifications and erased one year after their creation, unless they are required for monitoring procedures that have already begun in which case they shall be erased once the monitoring procedures no longer require these logs .	
348	7. eu-LISA shall keep the logs related to the history of the data stored in individual file, for purposes defined in paragraph 6. The logs related to the history of the data stored shall be erased once the data is erased.	7. eu-LISA shall keep the logs related to the history of the data stored in individual file, for purposes defined in paragraph 6. The logs related to the history of the data stored shall be erased automatically once the data is erased.	7. eu-LISA shall keep the logs related to the history of the data stored in individual file, for purposes defined in paragraph 6. eu-LISA shall erase the logs related to the history of the data stored shall be erased once the data are is erased.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
349		<i>7 a. The competent national authorities in charge of checking whether or not access is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning, data integrity and security, shall have access, within the limits of their competence and at their request, to the logs for the purpose of fulfilling their duties.</i>		
350		<i>7b. For the purposes of self-monitoring and ensuring the proper functioning of the CIR, data integrity and security, the eu-LISA shall have access, within the limits of its competence, to the logs.</i>		
351		<i>7c. The European Data Protection Supervisor shall have access, within the limits of its competence and upon request, to those logs for the purpose of fulfilling its tasks.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
352	CHAPTER V Multiple-identity Detector	CHAPTER V Multiple-identity Detector	CHAPTER V Multiple-identity Detector	
353	<i>Article 25 Multiple-identity detector</i>	<i>Article 25 Multiple-identity detector</i>	<i>Article 25 Multiple-identity detector</i>	
354	1. A multiple-identity detector (MID) creating and storing links between data in the EU information systems included in the common identity repository (CIR) and the SIS and as a consequence detecting multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud, is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, the VIS, the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system].	1. A multiple-identity detector (MID) creating and storing links between data in the EU Union information systems included in the common identity repository (CIR) and the SIS and as a consequence detecting multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud, is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, the VIS, the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system], while fully respecting the principles of necessity and proportionality.	1. A multiple-identity detector (MID) creating and storing <i>an identity confirmation file containing</i> links between data in the EU information systems included in the common identity repository (CIR) and the SIS and as a consequence detecting multiple identities, with the dual purpose of facilitating identity checks and combating identity fraud, is established for the purpose of supporting the functioning of the CIR and the objectives of the EES, the VIS, the ETIAS], Eurodac, the SIS and [the ECRIS-TCN system].	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
355	2. The MID shall be composed of:	2. The MID shall be composed of:	2. The MID shall be composed of:	
356	(a) a central infrastructure, storing links and references to information systems;	(a) a central infrastructure, storing links and references to information systems;	(a) a central infrastructure, storing links and references to <i>EU</i> information systems;	
357	(b) a secure communication infrastructure to connect the MID with the SIS and the central infrastructures of the European search portal and the CIR.	(b) a secure communication infrastructure to connect the MID with the SIS and the central infrastructures of the European search portal and the CIR.	(b) a secure communication infrastructure to connect the MID with the SIS and the central infrastructures of the European search portal and the CIR.	
358	3. eu-LISA shall develop the MID and ensure its technical management.	3. eu-LISA shall develop the MID and ensure its technical management. <i>It shall not have access to any of the personal data processed through the MID.</i>	3. eu-LISA shall develop the MID and ensure its technical management.	
359		<i>3a. eu-LISA and the competent authorities of the Member States shall use appropriate procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents discriminatory effects on natural persons on the basis of social, racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such effect.</i>		
360	<i>Article 26 Access to the multiple-identity detector</i>	<i>Article 26 Access to the multiple-identity detector</i>	<i>Article 26 Access to the multiple-identity detector</i>	
361	1. For the purposes of the manual identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:	1. For the purposes of the manual identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:	1. For the purposes of the manual identity verification referred to in Article 29, access to the data referred to in Article 34 stored in the MID shall be granted to:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
362	(a) border authorities when creating or updating an individual file as provided for in Article 14 of the [EES Regulation];	(a) border authorities when creating or updating an individual file as provided for in Article 14 of the [EES Regulation];	(a) border competent authorities referred to in Article 9(2) of Regulation (EU) 2017/2226 when creating or updating an individual file in EES in accordance with as provided for in Article 14 of that the [EES Regulation];	
363	(b) competent authorities referred to in Article 6(1) and (2) of Regulation 767/2008 when creating or updating an application file in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) competent authorities referred to in Article 6(1) and (2) of Regulation 767/2008 when creating or updating an application file in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) competent authorities referred to in Article 6(1) and (2) of Regulation 767/2008 when creating or updating an application file in the VIS in accordance with Article 8 of that Regulation (EC) No 767/2008;	
364	(c) [the ETIAS Central Unit and the ETIAS National Units when carrying out the assessment referred to in Articles 20 and 22 of the ETIAS Regulation;]	(c) [the ETIAS Central Unit and the ETIAS National Units when carrying out the assessment referred to in Articles 20 and 22 of the ETIAS Regulation;]	(c) [the ETIAS Central Unit and the ETIAS National Units when carrying out the assessment referred to in Articles 22 20 and 26 22 of the ETIAS Regulation;]	
365	(d) – (not applicable);	(d) (not applicable);	(d) (not applicable);	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
366	(e) the SIRENE Bureaux of the Member State creating a [SIS alert in accordance with the Regulation on SIS in the field of border checks];	(e) the SIRENE Bureaux of the Member State creating <i>or updating</i> a [SIS alert in accordance with the Regulation on SIS in the field of border checks];	(e) the SIRENE Bureaux of the Member State creating <i>or updating</i> a [SIS alert in accordance with the Regulation on SIS in the field of border checks <i>or Regulation on SIS for the return of illegally staying third-country nationals</i>];	
367	(f) – (not applicable).	(f) – (not applicable).	(f) – (not applicable).	
368	2. Member State authorities and EU bodies having access to at least one EU information system included in the common identity repository or to the SIS shall have access to the data referred to in Article 34(a) and (b) regarding any red links as referred to in Article 32.	2. Member State authorities and EU bodies having access to at least one EU information system included in the common identity repository or to the SIS shall have access to the data referred to in Article 34(a) and (b) regarding any red links as referred to in Article 32.	2. Member State authorities and EU <i>agencies</i> bodies having access to at least one EU information system included in the common identity repository <i>CIR</i> or to the SIS shall have access to the data referred to in Article 34(a) and (b) regarding any red links as referred to in Article 32.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
369	<i>Article 27 Multiple-identity detection</i>	<i>Article 27 Multiple-identity detection</i>	<i>Article 27 Multiple-identity detection</i>	
370	1. A multiple-identity detection in the common identity repository and the SIS shall be launched where:	1. A multiple-identity detection in the common identity repository and the SIS shall be launched where:	1. A multiple-identity detection in the common identity repository CIR and the SIS shall be launched where:	
371	(a) an individual file is created or updated in [the EES in accordance with Article 14 of the EES Regulation];	(a) an individual file is created or updated in [the EES in accordance with Article 14 of the EES Regulation];	(a) an individual file is created or updated in [the EES in accordance with Article 14 of the EES Regulation (EU) 2017/2226];	
372	(b) an application file is created or updated in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) an application file is created or updated in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) an application file is created or updated in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008	
373	(c) [an application file is created or updated in the ETIAS in accordance with Article 17 of the ETIAS Regulation;]	(c) [an application file is created or updated in the ETIAS in accordance with Article 17 of the ETIAS Regulation;]	(c) [an application file is created or updated in the ETIAS in accordance with Article 17 of the ETIAS Regulation;]	
374	(d) – (not applicable);	(d) — (not applicable);	(d) — (not applicable);	
375	(e) [an alert on a person is created or updated in the SIS in accordance with Chapter V of the Regulation on SIS in the field of	(e) [an alert on a person is created or updated in the SIS in accordance with Chapter V of the Regulation on SIS in the field of	(e) [an alert on a person is created or updated in the SIS in accordance with Chapter V of the Regulation on SIS in the field of	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	border checks];	border checks];	border checks <i>and Article 3 of the Regulation on SIS for the return of illegally staying third-country nationals</i> ;];	
376	(f) – (not applicable).	(f) – (not applicable).	(f) – (not applicable).	
377	2. Where the data contained within an information system as referred to in paragraph 1 contains biometric data, the common identity repository (CIR) and the Central-SIS shall use the shared biometric matching service (shared BMS) in order to perform the multiple-identity detection. The shared BMS shall compare the biometric templates obtained from any new biometric data to the biometric templates already contained in the shared BMS in order to verify whether or not data belonging to the same third-country national is already stored in the CIR or in the Central SIS.	2. Where the data contained within an information system as referred to in paragraph 1 contains biometric data, the common identity repository (CIR) and the Central SIS shall use the shared biometric matching service (shared BMS) in order to perform the multiple-identity detection. The shared BMS shall compare the biometric templates obtained from any new biometric data to the biometric templates already contained in the shared BMS in order to verify whether or not data belonging to the same third-country national person is already stored in the CIR or in the Central SIS.	2. Where the data contained within an <i>EU</i> information system as referred to in paragraph 1 contains biometric data, the common identity repository (CIR) and the Central-SIS shall use the shared biometric matching service (shared BMS) in order to perform the multiple-identity detection. The shared BMS shall compare the biometric templates obtained from any new biometric data to the biometric templates already contained in the shared BMS in order to verify whether or not data belonging to the same third-country national person is already stored in the CIR or in the Central SIS.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
378	3. In addition to the process referred to in paragraph 2, the CIR and the Central-SIS shall use the European search portal to search the data stored in the CIR and the Central-SIS using the following data:	3. In addition to the process referred to in paragraph 2, the CIR and the Central-SIS shall use the European search portal to search the data stored in the CIR and the Central-SIS using the following data:	3. In addition to the process referred to in paragraph 2, the CIR and the Central-SIS shall use the European search portal to search the data stored in the CIR and the Central-SIS and the CIR respectively using the following data:	
379	(a) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 16(1)(a) of the [EES Regulation];	(a) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 16(1)(a) of the [EES Regulation];	(a) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 16(1)(a) as well as the relevant data referred to in Articles 17(1) and 18(1) of the [EES Regulation (EU) 2017/2226] ;	
380	(b) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 9(4)(a) of Regulation (EC) No 767/2008;	(b) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 9(4)(a) of Regulation (EC) No 767/2008;	(b) surname (family name); first name(s) (given name(s)); date of birth, sex and nationality(ies) as referred to in Article 9(4)(a) of Regulation (EC) No 767/2008;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
381	(c) [surname (family name); first name(s) (given name(s)); surname at birth; date of birth, place of birth, sex and nationality(ies) as referred to in Article 15(2) of the ETIAS Regulation;]	(c) [surname (family name); first name(s) (given name(s)); surname at birth; date of birth, place of birth, sex and nationality(ies) as referred to in Article 15(2) of the ETIAS Regulation;]	(c) [surname (family name); first name(s) (given name(s)); surname at birth; <i>alias(es)</i> , date of birth, place of birth, sex and nationality(ies) as referred to in Article 17 15(2) of the ETIAS Regulation;]	
382	(d) – (not applicable);	(d) — (not applicable);	(d) — (not applicable);	
383	(e) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 20(2) of the Regulation on SIS in the field of border checks;]	(e) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 20(2) of the Regulation on SIS in the field of border checks;]	(e) [surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and <i>gender</i> sex as referred to in Article 20(2) of the Regulation on SIS in the field of border checks;]	
384	(f) – (not applicable);	(f) — (not applicable);	(f) — (not applicable);	
385	(g) – (not applicable);	(g) — (not applicable);	(g) [<i>surname(s); forename(s); name(s) at birth, previously used names and aliases; date of birth, place of birth, nationality(ies) and sex as referred to in Article 4 of the Regulation on SIS for the return of illegally staying third-country</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>nationals;]</i> (not applicable);	
386	(h) – (not applicable).	(h) – (not applicable).	(h) – (not applicable).	
387			<i>3a. In addition to the process referred to in paragraphs 2 and 3, the CIR and the Central-SIS shall use the European search portal to search the data stored in the Central-SIS and the CIR respectively using travel document data.</i>	
388	4. The multiple-identity detection shall only be launched in order to compare data available in one information system with data available in other information systems.	4. The multiple-identity detection shall only be launched in order to compare data available in one Union information system with data available in other Union information systems.	4. The multiple-identity detection may shall only be launched only in order to compare data available in one EU information system with data available in other EU information systems.	
389	<i>Article 28 Results of the multiple-identity detection</i>	<i>Article 28 Results of the multiple-identity detection</i>	<i>Article 28 Results of the multiple-identity detection</i>	
390	1. Where the queries referred to in Article 27(2) and (3) do not report any hit, the procedures referred to in Article 27(1) shall continue in	1. Where the queries referred to in Article 27(2) and (3) do not report any hit, the procedures referred to in Article 27(1) shall continue in	1. Where the queries referred to in Article 27(2), (3) and (3a) do not report any match hit , the procedures referred to in Article 27(1) shall continue in	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	accordance with the respective Regulations governing them.	accordance with the respective Regulations governing them.	accordance with the respective Regulations governing them.	
391	2. Where the query laid down in Article 27(2) and (3) reports one or several hit(s), the common identity repository and, where relevant, the SIS shall create a link between the data used to launch the query and the data triggering the hit.	2. Where the query laid down in Article 27(2) and (3) reports one or several hit(s), the common identity repository and, where relevant, the SIS shall create a link between the data used to launch the query and the data triggering the hit.	2. Where the query laid down in Article 27(2), (3) and (3a) reports one or several <i>match(es)</i> hit(s) , the common identity repository and, where relevant, the SIS shall create a link between the data used to launch the query and the data triggering the <i>match</i> hit .	
392	Where several hits are reported, a link shall be created between all data triggering the hit. Where data was already linked, the existing link shall be extended to the data used to launch the query.	Where several hits are reported, a link shall be created between all data triggering the hit. Where data was already linked, the existing link shall be extended to the data used to launch the query.	Where several <i>matches</i> hits are reported, a link shall be created between all data triggering the <i>match</i> hit . Where data was already linked, the existing link shall be extended to the data used to launch the query.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
393	3. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.	3. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.	3. Where the query referred to in Article 27(2), (3) and (3a) reports one or several hit(s) match(es) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article	
394	4. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.	4. Where the query referred to in Article 27(2) or (3) reports one or several hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.	4. Where the query referred to in Article 27(2), (3) and (3a) reports one or several match(es) hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.	
395	5. The Commission shall lay down the procedures to determine the cases where identity data can be considered as identical or similar in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to	5. The Commission shall lay down the procedures to determine the cases where identity data can be considered as identical or similar in implementing delegated acts. Those implementing acts delegated act shall be adopted in accordance with the examination procedure	5. The Commission shall lay down the procedures to determine the cases where identity data can be considered as the same identical , or similar or presenting some differences in implementing acts. Those implementing acts shall be adopted in accordance with the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	in Article 64(2).	referred to in Article 64(2) 63. <i>Such acts shall be designed in a manner that ensures the protection of persons with multiple lawful identities against discrimination.</i>	examination procedure referred to in Article 64(2).	
396			5a. <i>The Commission shall lay down the procedures to determine the cases where biometric data can be considered as the same in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).</i>	
397	6. The links shall be stored in the identity confirmation file referred to in Article 34.	6. The links shall be stored in the identity confirmation file referred to in Article 34.	6. The links shall be stored in the identity confirmation file referred to in Article 34.	
398	The Commission shall lay down the technical rules for linking data from different information systems by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	The Commission shall, <i>in cooperation with eu-LISA</i> , lay down the technical rules for linking data from different Union information systems by implementing acts. Those implementing acts shall be adopted in accordance with the	7. The Commission shall lay down the technical rules for linking data creating links between data from different EU information systems by implementing acts. Those implementing acts shall be adopted in accordance with the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		examination procedure referred to in Article 64(2).	examination procedure referred to in Article 64(2).	
399	<i>Article 29 Manual verification of different identities</i>	<i>Article 29 Manual verification of different identities</i>	<i>Article 29 Authorities responsible and manual verification of different identities</i>	
400	1. Without prejudice to paragraph 2, the authority responsible for verification of different identities shall be:	1. Without prejudice to paragraph 2, the authority responsible for verification of different identities shall be:	1. Without prejudice to paragraph 2, the authority responsible for verification of different identities shall be:	
401	(a) the border authority for hits that occurred when creating or updating an individual in [the EES in accordance with Article 14 of the EES Regulation];	(a) the border authority for hits that occurred when creating or updating an individual in [the EES in accordance with Article 14 of the EES Regulation];	(a) the border competent authority referred to in Article 9(2) of Regulation (EU) 2017/2226 for hits matches that occurred when creating or updating an individual file in [the EES in accordance with Article 14 of that the EES Regulation];	
402	(b) the competent authorities referred to in Article 6(1) and (2) of Regulation 767/2008 for hits that occurred when creating or updating an application file in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) the competent authorities referred to in Article 6(1) and (2) of Regulation 767/2008 for hits that occurred when creating or updating an application file in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) the competent authorities referred to in Article 6(1) and (2) of Regulation 767/2008 for hits matches that occurred when creating or updating an application file in the VIS in accordance with Article 8 of	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			Regulation (EC) No 767/2008;	
403	(c) [the ETIAS Central Unit and the ETIAS National Units for hits that occurred in accordance with Articles 18, 20 and 22 of the ETIAS Regulation;]	(c) [the ETIAS Central Unit and the ETIAS National Units for hits that occurred in accordance with Articles 18, 20 and 22 of the ETIAS Regulation;]	(c) [the ETIAS Central Unit and the ETIAS National Units for hits matches that occurred when creating or updating an application file in accordance with Articles 18, 20 and 22 of the ETIAS Regulation;]	
404	(d) – (not applicable);	(d) – (not applicable);	(d) – (not applicable);	
405	(e) the SIRENE Bureaux of the Member State for hits that occurred when creating a SIS alert in accordance with the [Regulations on SIS in the field of border checks];	(e) the SIRENE Bureaux of the Member State for hits that occurred when creating or updating a SIS alert in accordance with the [Regulations on SIS in the field of border checks];	(e) the SIRENE Bureaux of the Member State for hits matches that occurred when creating or updating a SIS alert in accordance with the [Regulations on SIS in the field of border checks and on SIS for the return of illegally staying third-country nationals];	
406	(f) – (not applicable).	(f) – (not applicable).	(f) – (not applicable).	
407	The multiple-identity detector shall indicate the authority responsible for the verification of different identities in the identity verification file.	The multiple-identity detector shall indicate the authority responsible for the verification of different identities in the identity verification file.	The multiple-identity detector shall indicate the authority responsible for the verification of different identities in the identity verification confirmation file.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
408	2. The authority responsible for the verification of different identities in the identity confirmation file shall be the SIRENE Bureau of the Member State that created the alert where a link is created to data contained:	2. The authority responsible for the verification of different identities in the identity confirmation file shall be the SIRENE Bureau of the Member State that created the alert where a link is created to data contained:	2. The authority responsible for the verification of different identities in the identity confirmation file shall be the SIRENE Bureau of the Member State that created the alert where a link is created to data contained:	
409	(a) in an alert in respect of persons wanted for arrest or for surrender or extradition purposes as referred to in Article 26 of [the Regulation on SIS in the field of law enforcement];	(a) in an alert in respect of persons wanted for arrest or for surrender or extradition purposes as referred to in Article 26 of [the Regulation on SIS in the field of law enforcement];	(a) in an alert in respect of persons wanted for arrest or for surrender or extradition purposes as referred to in Article 26 of [the Regulation on SIS in the field of law enforcement <i>police cooperation and judicial cooperation in criminal matters</i>];	
410	(b) in an alert on missing or vulnerable persons as referred to in Article 32 of [the Regulation on SIS in the field of law enforcement];	(b) in an alert on missing or vulnerable persons as referred to in Article 32 of [the Regulation on SIS in the field of law enforcement];	(b) in an alert on missing or vulnerable persons as referred to in Article 32 of [the Regulation on SIS in the field of law enforcement <i>police cooperation and judicial cooperation in criminal matters</i>];	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
411	(c) in an alert on persons sought to assist with a judicial procedure as referred to in Article 34 of [the Regulation on SIS in the field of law enforcement];	(c) in an alert on persons sought to assist with a judicial procedure as referred to in Article 34 of [the Regulation on SIS in the field of law enforcement];	(c) in an alert on persons sought to assist with a judicial procedure as referred to in Article 34 of [the Regulation on SIS in the field of law enforcement <i>police cooperation and judicial cooperation in criminal matters</i>];	
412	(d) [in an alert on return in accordance with the Regulation on SIS in the field of illegal return];	(d) [in an alert on return in accordance with the Regulation on SIS in the field of illegal return];	(d) [in an alert on return in accordance with the Regulation on SIS in the field of illegal return];	
413	(e) in an alert on persons for discreet checks, inquiry checks or specific checks as referred to in Article 36 of [the Regulation on SIS in the field of law enforcement];	(e) in an alert on persons for discreet checks, inquiry checks or specific checks as referred to in Article 36 of [the Regulation on SIS in the field of law enforcement];	(e) in an alert on persons for discreet checks, inquiry checks or specific checks as referred to in Article 36 of [the Regulation on SIS in the field of law enforcement <i>police cooperation and judicial cooperation in criminal matters</i>].	
414	(f) in an alert on unknown wanted persons for identification according to national law and search with biometric data as referred to in Article 40 of [the Regulation on SIS in the field of law enforcement].	(f) in an alert on unknown wanted persons for identification according to national law and search with biometric data as referred to in Article 40 of [the Regulation on SIS in the field of law enforcement].	(f) in an alert on unknown wanted persons for identification according to national law and search with biometric data as referred to in Article 40 of [the Regulation on SIS in the field of law enforcement].	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
415		<i>2a. Where the SIRENE Bureau is responsible for manually verifying different identities but has not been involved in the addition of the new identity data which has given rise to a yellow link, it shall be informed immediately by the authority which added the new identity data. The SIRENE Bureau shall carry out the manual verification of the different identities as soon as possible.</i>		
416	3. Without prejudice to paragraph 4, the authority responsible for verification of different identities shall have access to the related data contained in the relevant identity confirmation file and to the identity data linked in the common identity repository and, where relevant, in the SIS, and shall assess the different identities and shall update the link in accordance with Articles	3. Without prejudice to paragraph 4, the authority responsible for verification of different identities shall have access to the related data contained in the relevant identity confirmation file and to the identity data linked in the common identity repository and, where relevant, in the SIS, and shall assess the different identities and shall update the link in accordance with Articles	3. Without prejudice to paragraph 4, the authority responsible for verification of different identities shall have access to the related data contained in the relevant identity confirmation file and to the identity data linked in the common identity repository and, where relevant, in the SIS and . It shall assess the different identities and shall update the link in accordance with Articles	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	31, 32 and 33 and add it to the identity confirmation file without delay.	31, 32 and 33 and add it to the identity confirmation file without delay, <i>in any case within 24 hours.</i>	31, 32 and 33 and add it to the identity confirmation file without delay.	
417	4. Where the authority responsible for the verification of different identities in the identity confirmation file is the border authority creating or updating an individual file in the EES in accordance with Article 14 of the EES Regulation, and where a yellow link is obtained, the border authority shall carry out additional verifications as part of a second-line check. During this second-line check, the border authorities shall have access to the related data contained in the relevant identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it to the identity confirmation file without delay.	4. Where the authority responsible for the verification of different identities in the identity confirmation file is the border authority creating or updating an individual file in the EES in accordance with Article 14 of the EES Regulation, and where a yellow link is obtained, the border authority shall carry out additional verifications as part of a second-line check. During this second-line check. <i>For that purpose only</i> , the border authorities shall have access to the related data contained in the relevant identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 <i>of this Regulation</i> and add it to the identity confirmation file without delay.	4. Where the authority responsible for the verification of different identities in the identity confirmation file is the border <i>competent authority referred to in Article 9(2) of Regulation (EU) 2017/2226</i> creating or updating an individual file in the EES in accordance with Article 14 of the EES Regulation (EU) 2017/2226 , and where a yellow link is <i>created</i> obtained , <i>that</i> the border authority shall carry out additional verifications as part of a second-line check. During this second-line check, <i>that</i> The That border authorityies shall have access to the related data contained in the relevant identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31 to 33 and add it	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			to the identity confirmation file without delay.	
418	5. Where more than one link is obtained, the authority responsible for the verification of different identities shall assess each link separately.	5. Where more than one link is obtained, the authority responsible for the verification of different identities shall assess each link separately.	5. Where more than one link is <i>created</i> obtained , the authority responsible for the verification of different identities shall assess each link separately.	
419		<i>5a. The verification of different identities under this Article shall, as a rule, take place in the presence of the person concerned who shall be offered the opportunity to explain the circumstances to the authority responsible, which shall take those explanations into account. Where the verification leads to the establishment of a red link, the person concerned shall receive a justification in writing.</i>		
420		<i>5b. The manual verification of different identities shall take place within 8 hours from the creation of a yellow link under Article 28(4).</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
421	6. Where data reporting a hit was already linked, the authority responsible for the verification of different identities shall take into account the existing links when assessing the creation of new links.	6. Where data reporting a hit was already linked, the authority responsible for the verification of different identities shall take into account the existing links when assessing the creation of new links.	6. Where data reporting a hit match was already linked, the authority responsible for the verification of different identities shall take into account the existing links when assessing the creation of new links.	
422		<i>6a. Prior to being authorised to verify identities, the staff of the authorities referred to in paragraphs 1 and 2 shall receive specific training on how to conduct the verification of different identities.</i>		
423	<i>Article 30 Yellow link</i>	<i>Article 30 Yellow link</i>	<i>Article 30 Yellow link</i>	
424	1. A link between data from two or more information systems shall be classified as yellow in any of the following cases:	1. A link between data from two or more information systems shall be classified as yellow in any of the following cases:	1. A link between data from two or more EU information systems shall be classified as yellow in any of the following cases:	
425	(a) the linked data shares the same biometric but different identity data and no manual verification of different identity	(a) the linked data shares the same biometric but different identity data and no manual verification of different identity	(a) the linked data shares the same biometric but different identity data and no manual verification of different identity	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	has taken place;	has taken place;	has taken place;	
426	(b) the linked data has different identity data and no manual verification of different identity has taken place.	(b) the linked data has different identity data, <i>there is no biometric data to compare</i> , and no manual verification of different identity has taken place;	(b) the linked data has different <i>some differences in the identity data or in travel document data</i> , and no manual verification of different identity has taken place <i>and at least one of the EU information systems does not have biometric data on the person</i> ;	
427		(ba) <i>the linked data have the same identity data but different biometric data and no manual verification of different identities has taken place.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
428			<i>(c) the linked data has same or similar identity data, the same travel document data, but different biometric data and no manual verification of different identity has taken place.</i>	
429	2. Where a link is classified as yellow in accordance with paragraph 1, the procedure laid down in Article 29 applies.	2. Where a link is classified as yellow in accordance with paragraph 1, the procedure laid down in Article 29 applies.	2. Where a link is classified as yellow in accordance with paragraph 1, the procedure laid down in Article 29 applies.	
430	<i>Article 31 Green link</i>	<i>Article 31 Green link</i>	<i>Article 31 Green link</i>	
431	1. A link between data from two or more information systems shall be classified as green where the linked data do not share the same biometric but have similar identity data and the authority responsible for the verification of different identities concluded it refers to two different persons.	1. A link between data from two or more information systems shall be classified as green where the linked data do not share the same biometric but have similar identity data and the authority responsible for the verification of different identities concluded it refers to two different persons.:	1. A link between data from two or more EU information systems shall be classified as green where the linked data do not share the same biometric data but have same or similar identity data and the authority responsible for the verification of different identities concluded it refers to two different persons.	
432		<i>(a) the linked data do not share the same biometric but have similar identity data and</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>the authority responsible for the verification of different identities concluded it refers to two different persons;</i>		
433		<i>(b) the linked data share the same biometric data and the authority responsible for the verification of different identities has concluded that it refers to two different persons.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
434	2. Where the common identity repository (CIR) or the SIS are queried and where a green link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data does not correspond to the same person. The queried information system shall reply indicating only the data of the person whose data was used for the query, without triggering a hit against the data that is subject to the green link.	2. Where the common identity repository (CIR) or the SIS are queried and where a green link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data does not correspond to the same person. The queried information system shall reply indicating only the data of the person whose data was used for the query, without triggering a hit against the data that is subject to the green link.	2. Where the common identity repository (CIR) or the SIS are queried and where a green link exists between two or more of the <i>EU</i> information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data does not correspond to the same person. The queried information system shall reply indicating only the data of the person whose data was used for the query, without triggering a hit against the data that is subject to the green link.	
435	<i>Article 32 Red link</i>	<i>Article 32 Red link</i>	<i>Article 32 Red link</i>	
436	1. A link between data from two or more information systems shall be classified as red in any of the following cases:	1. A link between data from two or more information systems shall be classified as red in any of the following cases:	1. A link between data from two or more <i>EU</i> information systems shall be classified as red in any of the following cases:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
437	(a) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person;	(a) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers <i>unlawfully</i> to the same person <i>in an unjustified manner</i> ;	(a) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person <i>in an unjustified manner</i> ;	
438	(b) the linked data has similar identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person.	(b) the linked data has similar identity data and the authority responsible for the verification of different identities concluded it refers <i>unlawfully</i> to the same person <i>in an unjustified manner</i> .	(b) the linked data has similar identity data and the authority responsible for the verification of different identities concluded it refers unlawfully to the same person.	
439			(c) <i>the linked data has different identity data, at least one of the EU information systems does not have biometric data on the person and the authority responsible for the verification of different identities concluded it refers to the same person in an unjustified manner</i> ;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
440			<i>(d) the linked data has same or similar identity data, the same travel document data, but different biometric data and the authority responsible for the verification of different identities concluded it refers to different persons in an unjustified manner.</i>	
441	2. Where the CIR or the SIS are queried and where a red link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law.	2. Where the CIR or the SIS are queried and where a red link exists between two or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law. <i>No legal consequence for the person or persons concerned shall derive solely from the existence of a red link.</i>	2. Where the CIR or the SIS are queried and where a red link exists between two or more of the <i>EU</i> information systems constituting the CIR or with the SIS, the multiple-identity detector shall reply indicating the data referred to in Article 34. Follow-up to a red link shall take place in accordance with Union and national law, <i>basing any legal consequence for the person only on the relevant data on that person and not on the red link itself.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
442	3. Where a red link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN System], the individual file stored in the CIR shall be updated in accordance with Article 19(1).	3. Where a red link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN System], the individual file stored in the CIR shall be updated in accordance with Article 19(1).	3. Where a red link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN System], the individual file stored in the CIR shall be updated in accordance with Article 19(±2).	
443	4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a red link is created, the authority responsible for verification of different identities shall inform the person of the presence of multiple unlawful identities.	4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], and Without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a red link is created, the authority responsible for verification of different identities shall inform the person of the presence of multiple unlawful identities in accordance with Articles 12, 13 and 14 of Regulation (EU) 2016/679 and	4. Where a red link is created following a manual verification of multiple identities between data from the EES, the VIS, [the ETIAS] or the Eurodac, Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised, where a red link is created, the authority responsible for verification of different	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>Article 13 of Directive (EU) 680/2016.</i>	identities shall inform the person of the presence of multiple unlawful <i>unjustified</i> identities.	
444			<i>4a. The information shall be given by means of a standard form by the authority responsible for verification of different identities. The Commission shall determine the content of that form and the modalities for the information by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).</i>	
445	5. Where a red link is created, the authority responsible for verification of different identities shall provide a reference to the authorities responsible for the data linked.	5. Where a red link is created, the authority responsible for verification of different identities shall provide a reference to the authorities responsible for the data linked.	5. — Where a red link is created, the authority responsible for verification of different identities shall provide a reference to the authorities responsible for the data linked.	
446		<i>5 a. Where a Member State authority or Union agency with access to the CIR or SIS obtains evidence showing that a red link</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p><i>recorded in the MID is incorrect or that the data processed in the MID, CIR and SIS were processed in breach of this Regulation, that authority shall, where the link relates to Union information systems either rectify or erase the link from the MID immediately, or where the link relates to SIS, inform the relevant SIRENE Bureau of the Member State that created the SIS alert immediately. That SIRENE Bureau shall verify the evidence provided by the Member State authority and rectify or erase the link from the MID immediately thereafter.</i></p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
447			<p>6. If a Member State authority has evidence to suggest that a red link recorded in the MID is factually inaccurate or not up-to-date or that data were processed in the MID, the CIR or the SIS in breach of this Regulation, it shall check the relevant data stored in the CIR and SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.</p>	
448	<p><i>Article 33</i> <i>White link</i></p>	<p><i>Article 33</i> <i>White link</i></p>	<p><i>Article 33</i> <i>White link</i></p>	
449	<p>1. A link between data from two or more information systems shall be classified as white in any of the following cases:</p>	<p>1. A link between data from two or more information systems shall be classified as white in any of the following cases:</p>	<p>1. A link between data from two or more EU information systems shall be classified as white in any of the following cases:</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
450	(a) the linked data shares the same biometric and the same or similar identity data;	(a) the linked data shares the same biometric and the same or similar identity data;	(a) the linked data shares the same biometric and the same or similar identity data;	
451	(b) the linked data shares the same or similar identity data and at least one of the information systems does not have biometric data on the person;	(b) the linked data shares the same or similar identity data and at least one of the information systems does not have biometric data on the person;	(b) the linked data shares the same or similar identity data, and <i>the same travel document data,</i> <i>and</i> at least one of the <i>EU</i> information systems does not have biometric data on the person;	
452			<i>(ba) the linked data shares the same or similar identity data and at least one of the EU information systems does not have biometric data on the person and the authority responsible for the verification of different identities concluded it refers to the same person having different identity data in a justified manner;</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
453	(c) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers to the same person legally having different identity data.	(c) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers to the same person legally having different identity data.	(c) the linked data shares the same biometric but different identity data and the authority responsible for the verification of different identities concluded it refers to the same person legally having different identity data <i>in a justified manner.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
454		<i>(ca) the linked data shares the same identity data and different biometric data and the authority responsible for the verification of different identities has concluded that it refers to the same person and their biometric data has changed due to injury, illness or another legitimate reason.</i>		
455	2. Where the CIR or the SIS are queried and where a white link exists between one or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data correspond to the same person. The queried information systems shall reply indicating, where relevant, all the linked data on the person, hence triggering a hit against the data that is subject to the white link, if the authority launching the query has access to the linked data under Union or national law.	2. Where the CIR or the SIS are queried and where a white link exists between one or more of the information systems constituting the CIR or with the SIS, the multiple-identity detector shall indicate that the identity data of the linked data correspond to the same person. The queried information systems shall reply indicating, where relevant, all the linked data on the person, hence triggering a hit against the data that is subject to the white link, if the authority launching the query has access to the linked data under Union or national law.	2. Where the CIR or the SIS are queried and where a white link exists between one two or more of the EU information systems constituting the CIR or with the SIS, the multiple-identity detector MID shall indicate that the identity data of the linked data correspond to the same person. The queried EU information systems shall reply indicating, where relevant, all the linked data on the person, hence triggering a hit match against the data that is subject to the white link, if the authority launching the query has access to the linked	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			data under Union or national law.	
456	3. Where a white link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system], the individual file stored in the CIR shall be updated in accordance with Article 19(1).	3. Where a white link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system], the individual file stored in the CIR shall be updated in accordance with Article 19(1).	3. Where a white link is created between data from the EES, the VIS, [the ETIAS], Eurodac or [the ECRIS-TCN system], the individual file stored in the CIR shall be updated in accordance with Article 19(1 2).	
457	4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], where a white link is created following a manual verification of multiple identities, the authority responsible for verification of different identities shall inform the person of the presence of discrepancies between his or her personal data between systems and shall provide a reference to the authorities responsible for the data linked.	4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return], where a white link is created following a manual verification of multiple identities, the authority responsible for verification of different identities shall inform the person of the presence of discrepancies between his or her personal data between systems and shall provide a reference to the authorities responsible for the data linked.	4. Without prejudice to the provisions related to the handling of alerts in the SIS referred to in the [Regulations on SIS in the field of border checks, on SIS in the field of law enforcement and on SIS in the field of illegal return]; W Where a white link is created following a manual verification of multiple identities <i>between data from the EES, the VIS, [the ETIAS] or Eurodac</i> , the authority responsible for <i>the</i> verification of different identities shall inform the person of the presence of discrepancies between his or her personal data between systems and shall provide a reference to the authorities responsible for the data linked.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
458		<p><i>4a. If a Member State authority has evidence to suggest that a white link recorded in the MID is factually inaccurate, not up-to-date or that data were processed in the MID or the Union information systems or SIS in breach of this Regulation, it shall check the relevant data stored in the Union information systems and SIS and shall, if necessary, rectify or erase the link from the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.</i></p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
459			<i>4a. The information shall be given by means of a standard form by the authority responsible for verification of different identities. The Commission shall determine the content of that form and the modalities for the information by implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).</i>	
460			<i>5. If a Member State authority has evidence to suggest that a white link recorded in the MID is factually incorrect or that data were processed in the MID, the CIR or the SIS in breach of this Regulation, it shall check the relevant data stored in the CIR and SIS and shall, if necessary, rectify the link in the MID without delay. That Member State authority shall inform the Member State responsible for the manual verification without delay.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
461	<i>Article 34 Identity confirmation file</i>	<i>Article 34 Identity confirmation file</i>	<i>Article 34 Identity confirmation file</i>	
462	The identity confirmation file shall contain the following data:	The identity confirmation file shall contain the following data:	The identity confirmation file shall contain the following data:	
463	(a) the links, including their description in form of colours, as referred to in Articles 30 to 33;	(a) the links, including their description in form of colours, as referred to in Articles 30 to 33;	(a) the links, including their description in form of colours, as referred to in Articles 30 to 33;	
464	(b) a reference to the information systems whose data is linked;	(b) a reference to the information systems whose data is linked;	(b) a reference to the <i>EU</i> information systems whose data is are linked;	
465	(c) a single identification number allowing to retrieve the data from the information systems of corresponding linked files;	(c) a single identification number allowing to retrieve the data from the information systems of corresponding linked files;	(c) a single identification number allowing to retrieve the data from the <i>EU</i> information systems of corresponding linked files in accordance with respective access rights under Union and national law;	
466	(d) where relevant, the authority responsible for the verification of different identities.	(d) where relevant, the authority responsible for the verification of different identities.	(d) where relevant, the authority responsible for the verification of different identities;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
467			(e) <i>date of creation or update of the link.</i>	
468	<i>Article 35 Data retention in the multiple-identity detector</i>	<i>Article 35 Data retention in the multiple-identity detector</i>	<i>Article 35 Data retention in the multiple-identity detector</i>	
469	The identity confirmation files and its data, including the links, shall be stored in the multiple-identity detector (MID) only for as long as the linked data is stored in two or more EU information systems.	The identity confirmation files and its data, including the links, shall be stored in the multiple-identity detector (MID) only for as long as the linked data is stored in two or more EU Union information systems. <i>Once this condition is no longer met, the identity confirmation files and their data, including all related links, shall be deleted automatically.</i>	<i>1. Without prejudice to paragraphs 2 and 3,</i> the identity confirmation files and its <i>their</i> data, including the links, shall be stored in the multiple-identity detector (MID) only for as long as the linked data <i>are</i> is -stored in two or more EU information systems <i>and be deleted thereafter in an automated manner.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
470			<p><i>2. Where a red link is created between data in the CIR, the identity confirmation files and their data, including the red link, shall be stored in the MID only for as long as the corresponding data are stored in at least one of the EU information systems from which the linked data originates and be deleted thereafter in an automated manner.</i></p>	
471			<p><i>3. Where a red link is created between data in the CIR and the SIS, the identity confirmation files and their data, including the red link, shall be stored in the MID only for as long as the corresponding data are stored in the SIS and be deleted thereafter in an automated manner.</i></p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
472	<i>Article 36 Keeping of logs</i>	<i>Article 36 Keeping of logs</i>	<i>Article 36 Keeping of logs</i>	
473	1. eu-LISA shall keep logs of all data processing operations within the MID. Those logs shall include, in particular, the following:	1. eu-LISA shall keep logs of all data processing operations within the MID. Those logs shall include, in particular , the following:	1. eu-LISA shall keep logs of all data processing operations within the MID. Those logs shall include, in particular , the following:	
474		(-a) the Member State authority launching the query;		
475	(a) the purpose of access of the user and his or her access rights;	(a) the purpose of access of the user and his or her access rights;	(a) the purpose of access of the user and his or her access rights;	
476	(b) the date and time of the query;	(b) the date and time of the query;	(b) the date and time of the query;	
477	(c) the type of data used to launch the query or queries;	(c) the type of data used to launch the query or queries;	(c) the type of data used to launch the query or queries;	
478	(d) the reference to the data linked;	(d) the reference to the data linked;	(d) the reference to the data linked;	
479	(e) the history of the identity confirmation file;	(e) the history of the identity confirmation file;	(e) the history of the identity confirmation file;	
480	(f) the identifying mark of the person who carried out the	(f) the identifying mark of the person who carried out the	(f) the identifying mark of the person who carried out the <i>query Member State or EU</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	query.	query.	<i>agency querying the MID.</i>	
481		<i>In addition, Member States shall keep logs of the unique user identity of the official performing the query.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
482	2. Each Member State shall keep logs of the staff duly authorised to use the MID.	2. Each Member State shall keep logs of the staff duly authorised to use the MID.	2. Each Member State shall keep logs of the <i>authority, the purpose of access and the</i> staff duly authorised to use the MID.	
483	3. The logs may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. The logs shall be protected by appropriate measures against unauthorised access and erased one year after their creation, unless they are required for monitoring procedures that have already begun. The logs related to the history of the identity confirmation file shall be erased once the data in the identity confirmation file is erased.	3. The logs may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, <i>for self-monitoring</i> , and for ensuring <i>the proper functioning and the data integrity and data</i> security pursuant to Article 42. <i>To that end, access to those logs shall be granted as appropriate to the data controllers identified pursuant to Article 40, to the national supervisory authorities referred to in Article 51 of Regulation (EU)2016/679 and Article 41 of Directive (EU) 2016/680, and to the European Data Protection Supervisor.</i> The logs shall be protected by appropriate measures against unauthorised access and erased one year <i>two years</i> after their	3. The logs <i>referred to in paragraphs 1 and 2</i> may be used only for data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security pursuant to Article 42. Those logs shall be <i>made available to the competent supervisory authority on request. They shall be</i> protected by appropriate measures against unauthorised access <i>and modification.</i> and <i>They shall be</i> erased <i>in an automated manner</i> one year after their creation, unless they are required for monitoring procedures that have already begun <i>in which case they shall be erased once the monitoring procedures no longer require those logs.</i> The logs related to the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p>creation, unless they are required for monitoring procedures that have already begun. The logs related to the history of the identity confirmation file shall be erased once the data in the identity confirmation file is erased.</p>	<p>history of the identity confirmation file shall be erased once the data in the identity confirmation file is erased</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
484	CHAPTER VI Measures supporting interoperability	CHAPTER VI Measures supporting interoperability	CHAPTER VI Measures supporting interoperability	
485	<i>Article 37 Data quality</i>	<i>Article 37 Data quality</i>	<i>Article 37 Data quality</i>	
486		<i>-1. Member States shall ensure that the quality of the data in the EES,[ETIAS], VIS, SIS, the shared BMS, the CIR and the MID are closely monitored in order to ensure that they meet the overall requirements for the proper functioning of the respective Union information systems and the interoperability components. Member States shall also ensure that all staff entering data in any of those Union information systems has received prior training on data quality.</i>		
487	1. eu-LISA shall establish automated data quality control mechanisms and procedures on the data stored in the EES, the	1. eu-LISA shall establish <i>as soon as possible</i> automated data quality control mechanisms and procedures on the data stored in	1. <i>Without prejudice to Member States' responsibilities with regard to the quality of data entered into the systems,</i> eu-	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>[ETIAS], the VIS, the SIS, the shared biometric matching service (shared BMS), the common identity repository (CIR) and the multiple-identity detector (MID).</p>	<p>the EES, [theETIAS], the VIS, the SIS, the shared biometric matching service (shared BMS), the common identity repository and (CIR) and the multiple-identity detector (MID). <i>Those automated data quality control mechanisms shall be adequately tested prior to the start of operations of the interoperability components under Article 62.</i></p>	<p>LISA shall establish automated data quality control mechanisms and procedures on the data stored in the EES, <i>the VIS</i>, the [ETIAS], the VIS, the SIS, the shared biometric matching service (shared BMS); <i>and</i> the common identity repository (CIR) and the multiple-identity detector (MID).</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
488	2. eu-LISA shall establish common data quality indicators and the minimum quality standards to store data in the EES, the [ETIAS], the VIS, the SIS, the shared BMS, the CIR and the MID.	2. eu-LISA shall establish common data quality indicators and the minimum quality standards to store data in the EES, [the ETIAS], the VIS, the SIS, the shared BMS, the CIR and the MID. <i>Only data fulfilling the minimum quality standards may be entered in the EES, [ETIAS], VIS, SIS, the shared BMS, the CIR and the MID.</i> <i>If an authority attempts to enter data not fulfilling the applicable minimum quality standards, it shall immediately receive an automated warning from the relevant Union information system that the data cannot be entered, suggesting methods for satisfying the minimum quality standards.</i>	2. eu-LISA shall establish implement mechanisms for evaluating the accuracy of the shared BMS , common data quality indicators and the minimum quality standards to store data in the EES, the VIS , the [ETIAS], the VIS , the SIS, the shared BMS, and the CIR and the MID .	
489	3. eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the	3. eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the	3. eu-LISA shall provide regular reports on the automated data quality control mechanisms and procedures and the common data quality indicators to the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned.	Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned. <i>eu-LISA shall also provide that report to the European Parliament and the Council upon request. No reports provided under this paragraph shall contain any personal data.</i>	Member States. eu-LISA shall also provide a regular report to the Commission covering the issues encountered and the Member States concerned.	
490	4. The details of the automated data quality control mechanisms and procedures and the common data quality indicators and the minimum quality standards to store data in the EES, the [ETIAS], the VIS, the SIS, the shared BMS, the CIR and the MID, in particular regarding biometric data, shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	4. The details of the automated data quality control mechanisms and procedures and the common data quality indicators and the minimum quality standards to store data in the EES, the [ETIAS], the VIS, the SIS, the shared BMS, the CIR and the MID, in particular regarding biometric data, shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	4. The details of the automated data quality control mechanisms and procedures, and the common data quality indicators and the minimum quality standards to store data in the EES, <i>the VIS</i> , the [ETIAS], the VIS , the SIS, the shared BMS, <i>and</i> the CIR and the MID , in particular regarding biometric data, shall be laid down in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
491	5. One year after the establishment of the automated data quality control mechanisms and procedures and common data quality indicators and every year thereafter, the Commission shall evaluate Member State implementation of data quality and shall make any necessary recommendations. The Member States shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and shall report on any progress against this action plan until it is fully implemented.	5. One year after the establishment of the automated data quality control mechanisms and procedures and common data quality indicators and every year thereafter, the Commission shall evaluate Member State implementation of data quality and shall make any necessary recommendations. The Member States shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and, <i>in particular, data quality issues deriving from erroneous data in existing Union information systems and in SIS.</i> <i>The Commission</i> shall report on any progress against this action plan until it is fully implemented.	5. One year after the establishment of the automated data quality control mechanisms and procedures, and common data quality indicators <i>and the minimum quality standards</i> and every year thereafter, the Commission shall evaluate Member State implementation of data quality and shall make any necessary recommendations. The Member States shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and shall <i>regularly</i> report on any progress against this action plan until it is fully implemented.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
492	The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007. ¹⁰³	The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor, the European Data Protection Board and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007. ¹⁰⁴	The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007. ¹⁰⁵	
493		<i>Article 37a Availability and response time for interrogation</i>		
494		<i>All interoperability components shall be developed and managed in such a way as to ensure fast, seamless, efficient, controlled access, their full availability as laid down in Article 53(1) and a</i>		

¹⁰³ Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

¹⁰⁴ Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

¹⁰⁵ Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>response time in line with the operational needs of the Member States' authorities.</i>		
495	<i>Article 38 Universal Message Format</i>	<i>Article 38 Universal Message Format</i>	<i>Article 38 Universal Message Format</i>	
496	1. The Universal Message Format (UMF) standard is hereby established. The UMF defines standards for certain content elements of cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs	1. The Universal Message Format (UMF) standard is hereby established. The UMF defines standards for certain content elements of cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home affairs	1. The Universal Message Format (UMF) standard is hereby established. The UMF defines standards for certain content elements of cross-border information exchange between information systems, authorities and/or organisations in the field of Justice and Home Affairs	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
497	2. The UMF standard shall be used in the development of the EES, the [ETIAS], , the European search portal, the CIR, the MID and, if appropriate, in the development by eu-LISA or any other EU body of new information exchange models and information systems in the area of Justice and Home Affairs.	2. The UMF standard shall be used in the development of the EES, [the ETIAS], the European search portal ESP , the CIR, the MID <i>where feasible</i> and, if appropriate, in the development by eu-LISA or any other EU body Union agency of new information exchange models and Union information systems in the area of Justice and Home Affairs.	2. The UMF standard shall be used in the development of the EES, the [ETIAS], the European search portal , the CIR, the MID and, if appropriate, in the development by eu-LISA or any other EU body agency of new information exchange models and information systems in the area of Justice and Home Affairs.	
498	3. The implementation of the UMF standard may be considered in the VIS, the SIS and in any existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs, developed by Member States or associated countries.	3. The implementation of the UMF standard may be considered in the VIS, the SIS and in any existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs, developed by Member States or associated countries.	3. The implementation of the UMF standard may be considered in the VIS, the SIS and in any existing or new cross-border information exchange models and information systems in the area of Justice and Home Affairs, developed by Member States or associated countries.	
499	4. The Commission shall adopt an implementing act to lay down and develop the UMF standard referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to	4. The Commission shall adopt an implementing act to lay down and develop the UMF standard referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to	4. The Commission shall adopt an implementing act to lay down and develop the UMF standard referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	in Article 64(2).	in Article 64(2).	in Article 64(2).	
500	<i>Article 39 Central repository for reporting and statistics</i>	<i>Article 39 Central repository for reporting and statistics</i>	<i>Article 39 Central repository for reporting and statistics</i>	
501	1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the EES, the VIS, [the ETIAS] and the SIS and to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes.	1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the EES, the VIS, [the ETIAS] and the SIS and to generate provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes.	1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the EES, the VIS, [the ETIAS] and the SIS, in accordance with the respective legal instruments, as well as the Schengen Evaluation Mechanism provided for in Regulation (EU) No 1053/2013 , and to generate cross-system statistical data and analytical reporting for policy, operational and data quality purposes.	
502	2. eu-LISA shall establish, implement and host the CRRS in its technical sites containing the data referred to in [Article 63 of the EES Regulation], Article 17 of Regulation (EC) No 767/2008, [Article 73 of the ETIAS Regulation] and [Article 54 of the	2. eu-LISA shall establish, implement and host the CRRS in its technical sites containing the data referred to in [Article 63 of the EES Regulation], Article 17 of Regulation (EC) No 767/2008, [Article 73 of the ETIAS Regulation] and [Article 54 of the	2. eu-LISA shall establish, implement and host the CRRS in its technical sites containing the data referred to in {Article 63 of the EES Regulation (EU) 2017/2226 }, Article 17 of Regulation (EC) No 767/2008, [Article 73 84 of the ETIAS	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p>Regulation on SIS in the field of border checks], logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the repository shall be granted by means of secured access through the Trans-European Services for Telematics between Administrations (TESTA) network service with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in [Article 63 of the EES Regulation], Article 17 of Regulation (EC) No 767/2008, [Article 73 of the ETIAS Regulation] and [Article 54 of the Regulation on SIS in the field of border checks],.</p>	<p>Regulation on SIS in the field of border checks], logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the repository shall be granted by means of secured access through the Trans-European Services for Telematics between Administrations (TESTA) network service with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in [Article 63 of the EES Regulation], Article 17 of Regulation (EC) No 767/2008, [Article 73 of the ETIAS Regulation] and [Article 54 of the Regulation on SIS in the field of border checks],.</p>	<p>Regulation] and [Article 54 of the Regulation on SIS in the field of border checks <i>and Article 16 of the Regulation on the use of SIS for the return of illegally staying third-country nationals</i>], logically separated. The data contained in the CRRS shall not enable the identification of individuals. Access to the repository <i>CRRS</i> shall be granted by means of secured access through the Trans-European Services for Telematics between Administrations (TESTA) network service with control of access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in {Article 63 of the EES Regulation (<i>EU</i>) <i>2017/2226</i>}, Article 17 of Regulation (EC) No 767/2008, [Article 84 <i>73</i> of the ETIAS Regulation] and [Article 54 of the Regulation on SIS in the field of border checks],.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
503	3. eu-LISA shall render the data anonymous and shall record such anonymous data in the CRRS. The process for rendering the data anonymous shall be automated.	3. eu-LISA shall render the data anonymous, <i>by ensuring that the data subject is non-identifiable</i> , and shall record such anonymous data in the CRRS. The process for rendering the data anonymous shall be automated. <i>No access by eu-LISA staff shall be granted to any personal data stored in the Union information systems or in the interoperability components. The data contained in CRRS shall not allow for the identification of individuals.</i>	3. eu-LISA shall render the data anonymous and shall record such anonymous data in the CRRS. The process for rendering the data anonymous shall be automated.	
504	4. The CRRS shall be composed of:	4. The CRRS shall be composed of:	4. The CRRS shall be composed of:	
505			<i>(-a) the tools necessary for anonymising data;</i>	
506	(a) a central infrastructure, consisting of a data repository enabling the rendering of anonymous data;	(a) a central infrastructure, consisting of a data repository <i>and a mechanism that ensures for the data to be rendered enabling the rendering of anonymous data before it is</i>	(a) a central infrastructure, consisting of a data repository enabling the rendering of anonymous data;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>stored in CRRS;</i>		
507	(b) a secure communication infrastructure to connect the CRRS to the EES, [the ETIAS], the VIS and the SIS, as well as the central infrastructures of the shared BMS, the CIR and the MID.	(b) a secure communication infrastructure to connect the CRRS to the EES, [the ETIAS], the VIS and the SIS, as well as the central infrastructures of the shared BMS, the CIR and the MID.	(b) a secure communication infrastructure to connect the CRRS to the EES, <i>the VIS</i> , [the ETIAS], the VIS and the SIS, as well as the central infrastructures of the shared BMS, the CIR and the MID.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
508	<p>5. The Commission shall lay down detailed rules on the operation of the CRRS, including specific safeguards for processing of personal data referred to under paragraph 2 and 3 and security rules applicable to the repository by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).</p>	<p>5. The Commission shall lay down detailed rules on the operation of the CRRS, including specific safeguards for processing of personal data referred to under paragraph 2 and 3 and security rules applicable to the repository by means of <i>a delegated act</i> implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2) 63.</p>	<p>5. The Commission shall lay down detailed rules on the operation of the CRRS, including specific safeguards for processing of personal data referred to under paragraph 2 and 3 and security rules applicable to the repository by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
509	CHAPTER VII Data protection	CHAPTER VII Data protection	CHAPTER VII Data protection	
510	<i>Article 40 Data controller</i>	<i>Article 40 Data controller</i>	<i>Article 40 Data controller</i>	
511	1. In relation to the processing of data in the shared biometric matching service (shared BMS), the Member State authorities that are controllers for the VIS, EES, and SIS respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to the biometric templates obtained from the data referred to in Article 13 that they enter into respective systems and shall have responsibility for the processing of the biometric templates in the shared BMS.	1. In relation to the processing of data in the shared biometric matching service (shared BMS), the Member State authorities that are controllers for the VIS, EES, and SIS respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 <i>or Article 3(8) of Directive (EU) 2016/680</i> in relation to the biometric templates obtained from the data referred to in Article 13 that they enter into respective systems and shall have responsibility for the processing of the biometric templates in the shared BMS. <i>In relation to information security management of the shared BMS, eu-LISA shall be considered a</i>	1. In relation to the processing of data in the shared biometric matching service (shared BMS), the Member State authorities that are controllers for the VIS , EES, <i>the VIS</i> and SIS respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 <i>or Article 3(8) of Directive (EU) 2016/680</i> in relation to the biometric templates obtained from the data referred to in Article 13 that they enter into respective systems and shall have responsibility for the processing of the biometric templates in the shared BMS.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>controller.</i>		
512	2. In relation to the processing of data in the common identity repository (CIR), the Member State authorities that are controllers for the VIS, EES and [ETIAS], respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to data referred to in Article 18 that they enter into respective systems and shall have responsibility for the processing of that personal data in the CIR.	2. In relation to the processing of data in the common identity repository (CIR), the Member State authorities that are controllers for the VIS, EES and [ETIAS], respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to data referred to in Article 18 that they enter into respective systems and shall have responsibility for the processing of that personal data in the CIR.	2. In relation to the processing of data in the common identity repository (CIR), the Member State authorities that are controllers for the VIS , EES, <i>the VIS</i> and [ETIAS], respectively, shall also be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 in relation to data referred to in Article 18 that they enter into respective systems and shall have responsibility for the processing of that personal data in the CIR.	
513	3. In relation to the processing of data in the multiple-identity detector:	3. In relation to the processing of data in the multiple-identity detector:	3. In relation to the processing of data in the multiple-identity detector (<i>MID</i>):	
514	(a) the European Border and Coast Guard Agency shall be considered a data controller in accordance with Article 2(b) of Regulation No 45/2001 in relation to processing of personal data by the ETIAS Central Unit;	(a) the European Border and Coast Guard Agency shall be considered a data controller in accordance with Article 2(b) <i>2(d)</i> of Regulation (<i>EC</i>) No 45/2001 in relation to processing of personal data by the ETIAS	(a) the European Border and Coast Guard Agency shall be considered a data controller in accordance with Article 2(b) <i>(d)</i> of Regulation No 45/2001 [<i>or Article 3(2)(b) of Regulation XX/2018 of the European</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		Central Unit;	<i>Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]</i> in relation to <i>the</i> processing of personal data by the ETIAS Central Unit;	
515	(b) the Member State authorities adding or modifying the data in the identity confirmation file are also to be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 and shall have responsibility for the processing of the personal data in the multiple-identity detector;	(b) the Member State authorities adding or modifying the data in the identity confirmation file are also to be considered as controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 and shall have responsibility for the processing of the personal data in the multiple-identity detector;	(b) the Member State authorities adding or modifying the data in the identity confirmation file are also to be considered as <i>shall be</i> controllers in accordance with Article 4(7) of Regulation (EU) 2016/679 <i>or Article 3(8) of Directive (EU) 2016/680</i> and shall have responsibility for the processing of the personal data in the multiple-identity detector <i>MID</i> ;	
516		<i>3a. In relation to information security management of the interoperability components eu-</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>LISA shall be considered a data controller in accordance with Regulation (EC) No 45/2001.</i>		
517	<i>Article 41 Data processor</i>	<i>Article 41 Data processor</i>	<i>Article 41 Data processor</i>	
518	In relation to the processing of personal data in the CIR, eu-LISA is to be considered the data processor in accordance with Article 2(e) of Regulation (EC) No 45/2001.	In relation to the processing of personal data in the <i>shared BMS, the CIR and the MID</i> , eu-LISA is to be considered the data processor in accordance with Article 2(e) of Regulation (EC) No 45/2001.	In relation to the processing of personal data in <i>the shared BMS</i> , the CIR <i>and the MID</i> , eu-LISA shall is to be considered the data processor in accordance with Article 2(e) of Regulation (EC) No 45/2001 <i>[or Article 3(1)(a) of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]</i> .	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
519	<i>Article 42 Security of processing</i>	<i>Article 42 Security of processing</i>	<i>Article 42 Security of processing</i>	
520	1. Both eu-LISA and the Member State authorities shall ensure the security of the processing of personal data that takes place pursuant to the application of this Regulation. eu-LISA, [the ETIAS Central Unit] and the Member State authorities shall cooperate on security-related tasks.	1. Both eu-LISA, and the Member State authorities and Europol shall ensure the security of the processing of personal data that takes place pursuant to the application of this Regulation. eu-LISA, shall be responsible for the [the ETIAS central Unit] infrastructure of the interoperability components and Member States shall be responsible for the parts referred to in Article 54. eu-LISA, [the European Border and Coast Guard Agency], Europol and the Member State authorities shall cooperate on security-related tasks.	1. Both eu-LISA, [the ETIAS Central Unit], Europol and the Member State authorities shall ensure the security of the processing of personal data that takes place pursuant to the application of this Regulation. eu-LISA, [the ETIAS Central Unit], Europol and the Member State authorities shall cooperate on security-related tasks.	
521	2. Without prejudice to Article 22 of Regulation (EC) No 45/2001, eu-LISA shall take the necessary measures to ensure the security of the interoperability components and their related communication infrastructure.	2. Without prejudice to Article 22 of Regulation (EC) No 45/2001, eu-LISA shall take the necessary measures to ensure the security of the interoperability components and their related communication infrastructure.	2. Without prejudice to Article 22 of Regulation (EC) No 45/2001 [or Article 33 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC], eu-LISA shall take the necessary measures to ensure the security of the interoperability components and their related communication infrastructure.</i>	
522	3. In particular, eu-LISA shall adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:	3. In particular, eu-LISA shall adopt the necessary measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:	3. In particular, eu-LISA shall adopt the necessary <i>security</i> measures, including a security plan, a business continuity plan and a disaster recovery plan, in order to:	
523	(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;	(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;	(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;	
524		<i>(aa) deny unauthorised persons access to data-processing equipment and installations;</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
525	(b) prevent the unauthorised reading, copying, modification or removal of data media;	(b) prevent the unauthorised reading, copying, modification or removal of data media;	(b) prevent the unauthorised reading, copying, modification or removal of data media;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
526	(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;	(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;	(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;	
527	(d) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;	(d) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;	(d) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;	
528		<i>(da) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;</i>		
529	(e) ensure that persons authorised to access the interoperability components have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;	(e) ensure that persons authorised to access the interoperability components have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;	(e) ensure that persons authorised to access the interoperability components have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;	
530	(f) ensure that it is possible to verify and establish to which bodies personal data may be	(f) ensure that it is possible to verify and establish to which bodies personal data may be	(f) ensure that it is possible to verify and establish to which bodies personal data may be	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	transmitted using data communication equipment;	transmitted using data communication equipment;	transmitted using data communication equipment;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
531	(g) ensure that it is possible to verify and establish what data has been processed in the interoperability components, when, by whom and for what purpose;	(g) ensure that it is possible to verify and establish what data has been processed in the interoperability components, when, by whom and for what purpose;	(g) ensure that it is possible to verify and establish what data has been processed in the interoperability components, when, by whom and for what purpose;	
532	(h) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the interoperability components or during the transport of data media, in particular by means of appropriate encryption techniques;	(h) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the interoperability components or during the transport of data media, in particular by means of appropriate encryption techniques;	(h) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the interoperability components or during the transport of data media, in particular by means of appropriate encryption techniques;	
533		<i>(ha) ensure that, in the event of interruption, installed systems can be restored to normal operation;</i>		
534		<i>(hb) ensure reliability by making sure that any faults in the functioning of the interoperability components are properly reported;</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
535	(i) 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.	(i) 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 <i>and to assess those security measures in the light of new technological developments.</i>	(i) 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.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
536	4. Member States shall take measures equivalent to those referred to in paragraph 3 as regards security in respect of the processing of personal data by the authorities having a right to access any of the interoperability components.	4. Member States, <i>Europol and the European Border and Coast Guard Agency</i> shall take measures equivalent to those referred to in paragraph 3 as regards security in respect of the processing of personal data by the authorities having a right to access any of the interoperability components.	4. Member States, <i>[the ETIAS Central Unit] and Europol</i> shall take measures equivalent to those referred to in paragraph 3 as regards security in respect of the processing of personal data by the authorities having a right to access any of the interoperability components.	
537	<i>Article 43 Confidentiality of SIS data</i>	<i>Article 43 Confidentiality of SIS data</i>	<i>Article 43 Confidentiality of SIS data</i>	
538	1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.	1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.	1. Each Member State shall apply its rules of professional secrecy or other equivalent duties of confidentiality to all persons and bodies required to work with SIS data accessed through any of the interoperability components in accordance with its national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
539	2. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in paragraph 1 to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.	2. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in paragraph 1 <i>of this Article</i> to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.	2. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in paragraph 1 to all its staff required to work with SIS data. This obligation shall also apply after those persons leave office or employment or after the termination of their activities.	
540		<i>2a. Where eu-LISA or a Member State cooperates with external contractors in any task related to the interoperability components, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, in particular those on security, confidentiality and data protection.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
541	<i>Article 44 Security incidents</i>	<i>Article 44 Security incidents</i>	<i>Article 44 Security incidents</i>	
542	1. Any event that has or may have an impact on the security of the interoperability components and may cause damage to or loss of data stored in them shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.	1. Any event that has or may have an impact on the security of the interoperability components and may cause unauthorised access to , damage to or loss of data stored in them shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.	1. Any event that has or may have an impact on the security of the interoperability components and may cause damage to or loss of data stored in them shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.	
543	2. Security incidents shall be managed so as to ensure a quick, effective and proper response.	2. Security incidents shall be managed so as to ensure a quick, effective and proper response.	2. Security incidents shall be managed so as to ensure a quick, effective and proper response.	
544	3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States shall notify the	3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States and <i>Europa</i> shall notify	3. Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) 2016/679, Article 30 of Directive (EU) 2016/680, or both, Member States shall notify the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Commission, eu-LISA and the European Data Protection Supervisor of security incidents.	the Commission, eu-LISA, competent supervisory authorities and the European Data Protection Supervisor of any security incidents without delay . In the event of a security incident in relation to the central infrastructure of the interoperability components, eu-LISA shall notify the Commission and the European Data Protection Supervisor.	Commission, eu-LISA and the European Data Protection Supervisor of any security incidents.	
545		3a. The Commission shall report serious incidents immediately to the European Parliament and to the Council. Those reports shall be classified as EURESTRICTED/ RESTREINT UE in accordance with applicable security rules.		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
546			<i>Without prejudice to [Articles 34 and 35 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC] and Article 34 of Regulation (EU) 2016/794, [the ETIAS Central Unit] and Europol shall notify the Commission, eu-LISA and the European Data Protection Supervisor of any security incident.</i>	
547	In the event of a security incident in relation to the central infrastructure of the interoperability components, eu-LISA shall notify the Commission and the European Data Protection Supervisor.	In the event of a security incident in relation to the central infrastructure of the interoperability components, eu-LISA shall notify the Commission and the European Data Protection Supervisor.	In the event of a security incident in relation to the central infrastructure of the interoperability components, eu-LISA shall notify the Commission and the European Data Protection Supervisor.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
548	4. Information regarding a security incident that has or may have an impact on the operation of the interoperability components or on the availability, integrity and confidentiality of the data shall be provided to the Member States and reported in compliance with the incident management plan to be provided by eu-LISA.	4. Information regarding a security incident that has or may have an impact on the operation of the interoperability components or on the availability, integrity and confidentiality of the data shall be provided to the Member States, <i>the ETIAS Central Unit where necessary, and Europol without delay</i> and reported in compliance with the incident management plan to be provided by eu-LISA.	4. Information regarding a security incident that has or may have an impact on the operation of the interoperability components or on the availability, integrity and confidentiality of the data shall be provided to the Member States, <i>[the ETIAS Central Unit] and Europol</i> and reported in compliance with the incident management plan to be provided by eu-LISA.	
549	5. The Member States concerned and eu-LISA shall cooperate in the event of a security incident. The Commission shall lay down the specification of this cooperation procedure by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	5. The Member States concerned, <i>the ETIAS Central Unit, Europol</i> and eu-LISA shall cooperate in the event of a security incident. The Commission shall lay down the specification of this cooperation procedure by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	5. The Member States concerned, <i>[the ETIAS Central Unit], Europol</i> and eu-LISA shall cooperate in the event of a security incident. The Commission shall lay down the specification of this cooperation procedure by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
550	<i>Article 45 Self-monitoring</i>	<i>Article 45 Self-monitoring</i>	<i>Article 45 Self-monitoring</i>	
551	Member States and the relevant EU bodies shall ensure that each authority entitled to access the interoperability components takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority.	Member States and the relevant EU bodies Union agencies shall ensure that each authority entitled to access the interoperability components takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority.	Member States and the relevant EU bodies agencies shall ensure that each authority entitled to access the interoperability components takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority.	
552	The data controllers as referred to in Article 40 shall take the necessary measures to monitor the compliance of the data processing pursuant to this Regulation, including frequent verification of logs, and cooperate, where necessary, with the supervisory authorities referred to in Articles 49 and 50.	The data controllers as referred to in Article 40 shall take the necessary measures to monitor the compliance of the data processing pursuant to this Regulation, including frequent verification of logs, and cooperate, where necessary, with the supervisory authorities referred to in Articles 49 and 50.	The data controllers as referred to in Article 40 shall take the necessary measures to monitor the compliance of the data processing pursuant to this Regulation, including frequent verification of logs, and cooperate, where necessary, with the supervisory authorities referred to in Articles 49 and with the European Data Protection Supervisor as referred to in Article 50.	
553		<i>Article 45a</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>Penalties</i>		
554		<i>Member States shall ensure that any misuse of data, processing of data or exchange of data contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive and shall include the possibility for administrative and criminal penalties.</i>		
555		<i>Article 45b Liability</i>		
556		<i>1. Without prejudice to the right to compensation from, and liability of, the controller or processor under Regulations (EC) No 45/2001 and (EU) 2016/679 and Directive (EU) 2016/680:</i>		
557		<i>(a) any person or Member State that has suffered material or non-material damage as a result of an unlawful personal data</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>processing operation or any other act incompatible with this Regulation by a Member State shall be entitled to receive compensation from that Member State; and</i>		
558		<i>(b) any person or Member State that has suffered material or non-material damage as a result of any act by Europol, the European Border and Coast Guard Agency or eu-LISA incompatible with this Regulation shall be entitled to receive compensation from the agency in question.</i>		
559		<i>The Member State concerned, Europol, the European Border and Coast Guard Agency or eu-LISA shall be exempted from their liability under the first subparagraph, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.</i>		
560		<i>2. If any failure of a Member</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>State to comply with its obligations under this Regulation causes damage to the interoperability components, that Member State shall be liable for such damage, unless and insofar as eu-LISA or another Member State bound by this Regulation failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.</i>		
561		<i>3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of the defendant Member State. Claims for compensation against the controller or eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
562	<i>Article 46 Right of information</i>	<i>Article 46 Right of to information</i>	<i>Article 46 Right of information</i>	
563	1. Without prejudice to the right of information referred to in Articles 11 and 12 of Regulation (EC) 45/2001 and Articles 13 and 14 of Regulation (EU) 2016/679, persons whose data are stored in the shared biometric matching service, the common identity repository or the multiple-identity detector shall be informed by the authority collecting their data, at the time their data are collected, about the processing of personal data for the purposes of this Regulation, including about identity and contact details of the respective data controllers, and about the procedures for exercising their rights of access, rectification and erasure, as well as about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the	1. Without prejudice to the right of information referred to in Articles 11 and 12 of Regulation (EC) 45/2001 and Articles 13 and 14 of Regulation (EU) 2016/679, <i>The authority collecting the data of</i> persons whose data are stored in the shared biometric matching service <i>BMS</i> , the common identity repository <i>CIR</i> or the multiple identity detector <i>MID</i> shall be informed by <i>provide those persons with the information required under Articles 11 and 12 of Regulation, (EC) 45/2001 and Articles 13 and 14 of Regulation (EU) 2016/679 in the manner required by Article 12 and Article 13 of Directive 2016/680.</i> The authority collecting their data, <i>shall provide the information</i> at the time their <i>that such</i> data are collected, about the processing of personal data for the purposes	1. Without prejudice to the right of information referred to in Articles 11 and 12 of Regulation (EC) 45/2001 <i>[or Articles 15 and 16 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC], Articles 13 and 14 of Directive (EU) 2016/680</i> and Articles 13 and 14 of Regulation (EU) 2016/679, persons whose data are stored in the shared biometric matching service <i>BMS</i> , the common identity repository <i>CIR</i> or the multiple identity detector <i>MID</i> shall be informed by the authority collecting their data <i>data</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	collection of the data.	of this Regulation, including about identity and contact details of the respective data controllers, and about the procedures for exercising their rights of access, rectification and erasure, as well as about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the collection of the data.	<i>controller</i> , at the time their data are collected <i>in accordance with paragraph 2</i> , about the processing of personal data for the purposes of this Regulation, including about identity and contact details of the respective data controllers, <i>about the period for which the personal data will be stored or about the criteria used to determine that period</i> , and about the procedures for exercising their rights of access, rectification and erasure, as well as about the contact details of the European Data Protection Supervisor and of the national supervisory authority of the Member State responsible for the collection of the data.	
564		<i>1a. All information shall be provided to data subjects in a manner and language which they understand, or are reasonably expected to understand. This shall include providing information in a manner which is appropriate to</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>the age of the data subjects who are minors.</i>		
565	2. Persons whose data is recorded in the EES, the VIS or [the ETIAS] shall be informed about the processing of data for the purposes of this Regulation in accordance with paragraph 1 when:	2. Persons whose data is recorded in the EES, the VIS or [the ETIAS] shall be informed about the processing of data for the purposes of this Regulation in accordance with paragraph 1 when:	2. Persons whose data is <i>are</i> recorded in the EES, the VIS or [the ETIAS] shall be informed about the processing of <i>personal</i> data for the purposes of this Regulation in accordance with paragraph 1 when:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
566	(a) [an individual file is created or updated in the EES in accordance with Article 14 of the EES Regulation];	(a) [an individual file is created or updated in the EES in accordance with Article 14 of the EES Regulation];	(a) {an individual file is created or updated in the EES in accordance with Article 14 of the EES Regulation (<i>EU</i>) 2017/2226 };	
567	(b) an application file is created or updated in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) an application file is created or updated in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	(b) an application file is created or updated in the VIS in accordance with Article 8 of Regulation (EC) No 767/2008;	
568	(c) [an application file is created or updated in the ETIAS in accordance with Article 17 of the ETIAS Regulation;]	(c) [an application file is created or updated in the ETIAS in accordance with Article 17 of the ETIAS Regulation;]	(c) [an application file is created or updated in the ETIAS in accordance with Article 19 17 of the ETIAS Regulation;].	
569	(d) – (not applicable);	(d) — (not applicable);	(d) — (not applicable);	
570	(e) – (not applicable).	(e) — (not applicable).	(e) — (not applicable).	
571		Article 46a Information Campaign		
572		<i>The Commission shall, in cooperation with the supervisory authorities and the European Data Protection Supervisor, accompany the start of operations of each</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>interoperability component with an information campaign informing the public and, in particular, third-country nationals, about the objectives and the functioning of those components, the authorities having access and the conditions for such access, and the rights of persons concerned. Such information campaigns shall be conducted continuously.</i>		
573	<i>Article 47 Right of access, correction and erasure</i>	<i>Article 47 Right of access to, rectification, completion, correction and erasure of personal data, and of restriction of the processing thereof - web service</i>	<i>Article 47 Right of access, correction rectification and erasure of data stored in the MID</i>	
574	1. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 and Articles 15, 16, 17 and 18 of Regulation (EU) 2016/679, any person shall have the right to address him or herself to the Member State responsible for the manual verification of	1. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 and Articles 15, 16, 17 and 18 of Regulation (EU) 2016/679 and Articles 14 and 16 of Directive (EU) 2016/680 as regards the processing of personal data in the CIR, the	1. In order to exercise their rights under Articles 13, 14, 15 and 16 of Regulation (EC) 45/2001 [or Articles 17, 18, 19 and 20 of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	different identities or of any Member State, who shall examine and reply to the request.	<i>shared BMS and the MID</i> , any person shall have the right to address him or herself to the Member State responsible for the manual verification of different identities or of any <i>to any other</i> Member State, who shall examine and reply to the request.	<i>the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC], Article 16 of Directive (EU) 2016/680 and Articles 15, 16, 17 and 18 of Regulation (EU) 2016/679, any person shall have the right to address him or herself to the Member State responsible for the manual verification of different identities or <i>competent authority</i> of any Member State, who shall examine and reply to the request.</i>	
575		<i>1a. Without prejudice to paragraph 1, and in order to facilitate and better enable the effective exercise of the rights of data subjects as described in paragraph 1 to access, rectify, erase or restrict the processing of their personal data under interoperability components, in particular for those third-country nationals who may be</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p><i>outside the territory of the Member States, eu-LISA shall establish a web service, hosted in its technical site, which shall enable data subjects to make requests for access, correction, erasure or rectification of their personal data. The web service shall act as a single point of contact for those third-country nationals who are outside the territory of the Member States.</i></p> <p><i>The web service shall immediately transmit such requests to the Member State responsible for manual verification of different identities in accordance with Article 29 or, where appropriate, to the Member State responsible for the entry of the data in the underlying Union information system which is the subject of the request.</i></p>		
576		<p><i>1b. The Commission shall adopt implementing acts concerning the detailed rules on</i></p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>the conditions for the operation of the web service and the applicable data protection and security rules. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
577	2. The Member State responsible for the manual verification of different identities as referred to in Article 29 or the Member State to which the request has been made shall reply to such requests within 45 days of receipt of the request.	2. The Member State responsible for the manual verification of different identities as referred to in Article 29 or the Member State to which the request has been made, <i>either directly from the data subject in accordance with paragraph 1 or via the web service in accordance with paragraph 1a</i> , shall reply to such requests <i>without undue delay and in any event</i> within 45 days <i>one month</i> of receipt of the request.	2. The Member State responsible for the manual verification of different identities as referred to in Article 29 or the Member State to which the request has been made <i>The Member State which examined such request</i> shall reply to such requests within 45 <i>60</i> days of receipt of the request. <i>Member States may decide that these replies are given by central offices.</i>	
578	3. If a request for correction or erasure of personal data is made to a Member State other than the Member State responsible, the Member State to which the request has been made shall contact the authorities of the Member State responsible within seven days and the Member State responsible shall check the accuracy of the data and the lawfulness of the data processing within 30 days of such contact.	3. If a request for <i>access</i> , correction or erasure of personal data is made to a Member State other than the Member State responsible, the Member State to which the request has been made shall contact the authorities of the Member State responsible <i>in writing</i> within seven days and the Member State responsible shall check the accuracy of the data and the lawfulness of the data processing <i>without undue delay</i>	3. If a request for correction <i>rectification</i> or erasure of personal data is made to a Member State other than the Member State responsible <i>for the manual verification of different identities</i> , the Member State to which the request has been made shall contact the authorities of the Member State responsible <i>for the manual verification of different identities</i> within seven days. and € The Member State responsible	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>and in any event</i> within 30 days one month of such contact. <i>The person concerned shall be informed by the Member State which contacted the authority of the Member State responsible that his or her request was forwarded about the further procedure.</i>	<i>for the manual verification of different identities</i> shall check the accuracy of the data and the lawfulness of the data processing within 30 45 days of such contact.	
579			<i>3a. If a request for rectification or erasure of personal data is made to a Member State where the ETIAS Central Unit was responsible for the manual verification of different identities, the Member State to which the request has been made shall contact the ETIAS Central Unit within seven days and ask for its opinion to be given within 45 days of such contact.</i>	
580	4. Where, following an examination, it is found that the data stored in the multiple-identity detector (MID) are factually inaccurate or have been	4. Where, following an examination, it is found that the data stored in the multiple-identity detector (MID) CIR, the shared BMS and MID are	4. Where, following an examination, it is found that the data stored in the multiple-identity detector (MID) are factually inaccurate or have been	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	recorded unlawfully, the Member State responsible or, where applicable, the Member State to which the request has been made shall correct or delete these data.	factually inaccurate or have been recorded unlawfully, the Member State responsible or, where applicable, the Member State to which the request has been made shall <i>immediately</i> correct or delete these data. <i>The person concerned shall be informed in writing that his or her data has been rectified or erased.</i>	recorded unlawfully, the Member State responsible <i>for the manual verification of different identities</i> or, where <i>there was no Member State responsible for the manual verification or where the ETIAS Central Unit was responsible for the manual verification</i> applicable, the Member State to which the request has been made shall correct or delete these data.	
581		<i>4a. Any person shall have the right to lodge a complaint and the right to a legal remedy in the Member State which has refused the right of access to or the right of rectification or erasure of data relating to him or her, in accordance with Union or national law.</i>		
582	5. Where data in the MID is amended by the responsible Member State during its validity period, the responsible Member State shall carry out the processing laid down in Article 27 and, where relevant, Article 29	5. Where data <i>in the CIR, the shared BMS or</i> in the MID is amended by the responsible Member State during its validity period, the responsible Member State shall carry out the processing laid down in Article	5. Where data <i>stored</i> in the MID is amended by <i>a the responsible</i> Member State during its validity period, the responsible <i>that</i> Member State shall carry out the processing laid down in Article 27 and, where relevant,	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	to determine whether the amended data shall be linked. Where the processing does not report any hit, the responsible Member State or, where applicable, the Member State to which the request has been made shall delete the data from the identity confirmation file. Where the automated processing reports one or several hit(s), the responsible Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.	27 and, where relevant, Article 29 to determine whether the amended data shall be linked. Where the processing does not report any hit, the responsible Member State or, where applicable, the Member State to which the request has been made shall delete the data from the identity confirmation file. Where the automated processing reports one or several hit(s), the responsible Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.	Article 29 to determine whether the amended data shall be linked. Where the processing does not report any hit match , the responsible that Member State or, where applicable, the Member State to which the request has been made shall delete the data from the identity confirmation file. Where the automated processing reports one or several match(es) hit(s) , the responsible that Member State shall create or update the relevant link in accordance with the relevant provisions of this Regulation.	
583	6. Where the responsible Member State or, where applicable, the Member State to which the request has been made does not agree that data stored in the MID are factually inaccurate or have been recorded unlawfully, that Member State shall adopt an administrative decision explaining in writing to	6. Where the responsible Member State or, where applicable, the Member State to which the request has been made does not agree that data stored in the CIR, the shared BMS or the MID are factually inaccurate or have been recorded unlawfully, that Member State shall adopt an administrative decision	6. Where the responsible Member State responsible for the manual verification of different identities or, where applicable, the Member State to which the request has been made does not agree that data stored in the MID are factually inaccurate or have been recorded unlawfully, that Member State shall adopt an	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	the person concerned without delay why it is not prepared to correct or delete data relating to him or her.	explaining in writing to the person concerned without delay why it is not prepared to correct or delete data relating to him or her.	administrative decision explaining in writing to the person concerned without delay why it is not prepared to correct or delete data relating to him or her.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
584	7. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request referred in paragraph 3 and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts, and any assistance, including from the competent national supervisory authorities.	7. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request referred <i>to in paragraphs 1, 2 and</i> paragraph 3 and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts, and any assistance, including from the competent national supervisory authorities <i>together with its contact details.</i>	7. This decision shall also provide the person concerned with information explaining the possibility to challenge the decision taken in respect of the request <i>for rectification or erasure of personal data</i> referred in paragraph 3 and, where relevant, information on how to bring an action or a complaint before the competent authorities or courts, and any assistance, including from the competent national supervisory authorities.	
585	8. Any request made pursuant to paragraph 3 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 3 and shall be erased immediately afterwards.	8. Any request made pursuant to paragraph <i>paragraphs 1, 2 and</i> 3 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 3 and shall be erased immediately afterwards.	8. Any request <i>for rectification or erasure of personal data</i> made pursuant to paragraph 3 shall contain the necessary information to identify the person concerned. That information shall be used exclusively to enable the exercise of the rights referred to in paragraph 3 <i>this Article</i> and shall be erased immediately afterwards.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
586	9. The responsible Member State or, where applicable, the Member State to which the request has been made shall keep a record in the form of a written document that a request referred to in paragraph 3 was made and how it was addressed, and shall make that document available to competent data protection national supervisory authorities without delay.	9. The responsible Member State or, where applicable, the Member State to which the request has been made shall keep a record in the form of a written document that a request referred to in paragraph paragraphs 1, 2 and 3 was made and how it was addressed, and shall make that document available to competent data protection national supervisory authorities without delay.	9. The responsible Member State <i>responsible for the manual verification of different identities</i> or, where applicable, the Member State to which the request has been made shall keep a record in the form of a written document that a request <i>for rectification or erasure of personal data</i> referred to in paragraph 3 was made and how it was addressed, and shall make that document available to competent data protection national supervisory authorities without delay.	
587			<i>Article 47a¹⁰⁶ Penalties</i>	
588			<i>Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.</i>	

¹⁰⁶ Articles 47a and 47b are copied from the text agreed with the EP on the ETIAS Regulation.

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
589			<i>Article 47b Liability</i>	
590			<i>1. Without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and [Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC]:</i>	
591			<i>(a) any person or Member State that has suffered material or non-material damage as a result of an unlawful personal data processing operation or any other act incompatible with this Regulation by a Member State</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>shall be entitled to receive compensation from that Member State;</i>	
592			<i>(b) any person or Member State that has suffered material or non-material damage as a result of any act by eu-LISA incompatible with this Regulation shall be entitled to receive compensation from that agency. eu-LISA shall be liable for unlawful personal data processing operations in accordance with its role as processor.</i>	
593			<i>That Member State or eu-LISA shall be exempted from their liability, in whole or in part, if they prove that they are not responsible for the event which gave rise to the damage.</i>	
594			<i>2. If any failure of a Member State to comply with its obligations under this Regulation causes damage to the interoperability components, that</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>Member State shall be held liable for such damage, unless and insofar as eu-LISA or another Member State participating in the interoperability components failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.</i>	
595			<i>3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the national law of the defendant Member State. Claims for compensation against the controller or eu-LISA for the damage referred to in paragraphs 1 and 2 shall be subject to the conditions provided for in the Treaties.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
596	<i>Article 48 Communication of personal data to third countries, international organisations and private parties</i>	<i>Article 48 Communication of personal data to third countries, international organisations and private parties</i>	<i>Article 48 Communication of personal data to third countries, international organisations and private parties</i>	
597	Personal data stored in or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party, with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in [Article 18(2)(b) and (m) of the ETIAS Regulation] or for the purposes of Article 8(2) of Regulation (EU) 2016/399. Such transfers of personal data to Interpol shall be compliant with the provisions of Article 9 of Regulation (EC) No 45/2001 and Chapter V of Regulation (EU) 2016/679.	<i>Without prejudice to [Article 65 of the ETIAS Regulation], Article 41 of Regulation (EU) 2017/2226, Article 31 of Regulation (EC) No 767/2008, Article 25 of Regulation (EU) 2016/794 and the querying of Interpol databases through the ESP in accordance with Article 9(5) of this Regulation,</i> personal data stored in, <i>processed</i> or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party, with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in [Article 18(2)(b) and (m) of the ETIAS Regulation] or for the purposes of Article 8(2) of	<i>Without prejudice to [Article 65 of the ETIAS Regulation], Article 41 of Regulation (EU) 2017/2226, and Article 31 of Regulation (EC) 767/2008,</i> Personal data stored in or accessed by the interoperability components shall not be transferred or made available to any third country, to any international organisation or to any private party, with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in [Article 18(2)(b) and (m) of the ETIAS Regulation] or for the purposes of Article 8(2) of Regulation (EU) 2016/399. Such transfers of personal data to Interpol shall be compliant with the provisions of Article 9 of Regulation (EC) No 45/2001 <i>[or</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		Regulation (EU) 2016/399. Such transfers of personal data to Interpol shall be compliant with the provisions of Article 9 of Regulation (EC) No 45/2001 and Chapter V of Regulation (EU) 2016/679.	<i>Chapter V of Regulation XX/2018 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC] and Chapter V of Regulation (EU) 2016/679.</i>	
598		<i>Any breach of this Article shall be considered a serious security incident and shall be immediately reported and addressed in accordance with Article 44.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
599	<i>Article 49 Supervision by the national supervisory authority</i>	<i>Article 49 Supervision by the national supervisory authority</i>	<i>Article 49 Supervision by the national supervisory authorities</i>	
600		<i>-1. Each Member State shall ensure that the supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 independently monitors the lawfulness of the processing of personal data pursuant to this Regulation by the Member State concerned.</i>		
601		<i>-1a. Each Member State shall ensure that the national laws, regulations and administrative provisions adopted pursuant to Directive (EU) 2016/680 are also applicable to access to the interoperability components by police authorities and designated authorities, including in relation to the rights of the persons whose data are so accessed.</i>		
602		<i>-1b. The supervisory authority referred to in Article 41(1) of Directive (EU) 2016/680 shall</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>monitor the lawfulness of the access to personal data by the Member States police authorities and designated authorities. Article 49(2) and (2a) of this Regulation shall apply accordingly.</i>		
603	1. The supervisory authority or authorities designated pursuant to Article 49 of Regulation (EU) 2016/679 shall ensure that an audit of the data processing operations by the responsible national authorities is carried out in accordance with relevant international auditing standards at least every four years.	1. The supervisory authority or authorities designated pursuant to <i>referred to in Article 49 51(1)</i> of Regulation (EU) 2016/679 <i>or pursuant to Article 41 of Directive (EU) 2016/680</i> shall ensure that an audit of the data processing operations by the responsible national authorities is carried out in accordance with relevant international auditing standards at least every four years. <i>The first such audit shall be carried out two years after the date on which the last interoperability component starts operations under Article 62. The results of the audit may be taken into account in the evaluations conducted under the mechanism</i>	1. The supervisory authority or authorities designated pursuant to Article 49 of Regulation (EU) 2016/679 shall ensure that an audit of the <i>personal</i> data processing operations by the responsible national authorities <i>for the purposes of this Regulation</i> is carried out in accordance with relevant international auditing standards at least every four years.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>established by Council Regulation (EU) No 1053/2013¹⁰⁷. The supervisory authorities referred to in Article 51(1) of Regulation (EU) 2016/679 and Article 41(1) of Directive (EU) 2016/680 shall publish annually the number of requests for rectification, completion or erasure, or restriction of processing of data, the action subsequently taken and the number of rectifications, completions, erasures and restrictions of processing made in response to requests by the persons concerned.</i>		
604	2. Member States shall ensure that their supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.	2. Member States shall ensure that their supervisory authority has sufficient resources, including both human and financial resources , to fulfil the tasks entrusted to it under this	2. Member States shall ensure that their supervisory authority has authorities have sufficient resources to fulfil the tasks entrusted to it them under this Regulation.	

¹⁰⁷ Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		Regulation <i>and has access to advice from persons with sufficient knowledge of biometric data. Member States shall grant the supervisory authority access to their logs without prejudice to constraints imposed binational security interests.</i>		
605		<i>2a. Member States shall supply any information requested by a supervisory authority referred to in Article 51(1) of Regulation (EU) 2016/679 and shall, in particular, provide it with information on the activities carried out in accordance with their responsibilities as laid down in this Regulation. Member States shall grant the supervisory authorities referred to in Article 51(1) of Regulation (EU) 2016/679 access to their logs and allow them to access all their premises used for interoperability purposes at all</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>times.</i>		
606			<p>3. Each Member State shall ensure that the supervisory authority established in accordance with Article 51(1) of Regulation (EU) 2016/679 and Article 41(1) of Directive (EU) 2016/680 independently monitors the lawfulness of the processing of personal data referred to in this Regulation by the Member State concerned, including their transmission to and from the components of interoperability.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
607	<i>Article 50 Supervision by the European Data Protection Supervisor</i>	<i>Article 50 Supervision by the European Data Protection Supervisor</i>	<i>Article 50 Supervision Audit by the European Data Protection Supervisor</i>	
608	The European Data Protection Supervisor shall ensure that an audit of eu-LISA's personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, the Council, eu-LISA, the Commission and the Member States. eu-LISA shall be given an opportunity to make comments before the reports are adopted.	<i>The European Data Protection Supervisor shall be responsible for monitoring the personal data processing activities of eu-LISA, Europol and the European Border and Coast Guard Agency under this Regulation and for ensuring that such activities are carried out in accordance with Regulation (EC) No 45/2001, Regulation (EU) 2016/794 and with this Regulation. eu-LISA shall supply information requested by the European Data Protection Supervisor to it, give the European Data Protection Supervisor access to all the documents and to its logs referred to in Articles 10, 16, 24 and 36 and allow the European Data Protection Supervisor access to all its premises at any</i>	The European Data Protection Supervisor shall ensure that an audit of eu-LISA's personal data processing activities <i>operations by eu-LISA, [the ETIAS Central Unit] and Europol for the purposes of this Regulation</i> is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, the Council, eu-LISA, the Commission, and the Member States <i>and the EU agency concerned</i> . eu-LISA, <i>[the ETIAS Central Unit] and Europol</i> shall be given an opportunity to make comments before the reports are adopted.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p><i>time.</i></p> <p>The European Data Protection Supervisor shall ensure that an audit of eu-LISA’s personal data processing activities is carried out in accordance with relevant international auditing standards at least every four years. <i>The first such audit shall be carried out two years after the date on which the last interoperability component starts operations in accordance with Article 62.</i> A report of that audit shall be sent to the European Parliament, the Council, eu-LISA, the Commission and the Member States. eu-LISA shall be given an opportunity to make comments before the reports are adopted. <i>The European Data Protection Supervisor shall have sufficient additional resources, including both human and financial resources, to fulfil the tasks entrusted to it under this Regulation.</i></p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
609	<i>Article 51 Cooperation between national supervisory authorities and the European Data Protection Supervisor</i>	<i>Article 51 Cooperation between national supervisory authorities and the European Data Protection Supervisor</i>	<i>Article 51 Cooperation between national supervisory authorities and the European Data Protection Supervisor</i>	
610	1. The European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, in particular if the European Data Protection Supervisor or a national supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the interoperability components, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.	1. <i>The supervisory authorities and</i> the European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, <i>each acting within the scope of their respective competences, cooperate actively within the framework of their respective responsibilities and ensure coordinated supervision of the use of the interoperability components and the application of other provisions of this Regulation,</i> in particular if the European Data Protection Supervisor or a national supervisory authority finds major discrepancies between practices of Member States or finds	1. The European Data Protection Supervisor shall act in close cooperation with national supervisory authorities with respect to specific issues requiring national involvement, in particular if the European Data Protection Supervisor or a national supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the interoperability components, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p>potentially unlawful transfers using the communication channels of the interoperability components, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.</p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
611	2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) XXXX/2018 [revised Regulation 45/2001].	2. <i>The European Data Protection Supervisor and the supervisory authorities shall exchange relevant information, assist each other in carrying out audits and inspections, examine any difficulties concerning the interpretation or application of this Regulation, assess problems in the cases referred to in paragraph 1, coordinated exercise of independent supervision or in the exercise of the rights of the data subject, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary shall be ensured in accordance with Article 62 of Regulation (EU) XXXX/2018 [revised Regulation 45/2001].</i>	2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with [Article 61 62 of Regulation (EU) XXXX/2018 [revised Regulation 45/2001] of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC].	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
612		<p><i>2a. For the purpose of paragraph 2, the supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year within the framework of the European Data Protection Board established by Regulation (EU)2016/679 (the ‘European Data Protection Board’). The costs of those meetings shall be borne by that Board, which shall also organise them. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.</i></p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
613		<i>2b. The European Data Protection Board shall send a joint report of activities to the European Parliament, the Council, the Commission, Europol, the European Border and Coast Guard Agency and eu-LISA two years after entry into force of this Regulation and every two years thereafter. That report shall include a chapter on each Member State prepared by the supervisory authority of that Member State.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
614	CHAPTER VIII Responsibilities	CHAPTER VIII Responsibilities	CHAPTER VIII Responsibilities	
615	<i>Article 52 Responsibilities of eu-LISA during the design and development phase</i>	<i>Article 52 Responsibilities of eu-LISA during the design and development phase</i>	<i>Article 52 Responsibilities of eu-LISA during the design and development phase</i>	
616	1. eu-LISA shall ensure that the central infrastructures of the interoperability components are operated in accordance with this Regulation.	1. eu-LISA shall ensure that the central infrastructures of the interoperability components are operated in accordance with this Regulation.	1. eu-LISA shall ensure that the central infrastructures of the interoperability components are operated in accordance with this Regulation.	
617	2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed referred to in Article 53(1).	2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed referred to in Article 37, Article 37a and Article 53(1) .	2. The interoperability components shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and speed performance referred to in Article 53(1).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
618	3. eu-LISA shall be responsible for the development of the interoperability components, for any adaptations required for establishing interoperability between the central systems of the EES, VIS, [ETIAS], SIS, and Eurodac, and [the ECRIS-TCN system], and the European search portal, the shared biometric matching service, the common identity repository and the multiple-identity detector.	eu-LISA shall be responsible for the <i>design and</i> development of the interoperability components, for any adaptations required for establishing interoperability between the central systems of the EES, VIS, [ETIAS], SIS, and Eurodac, and [the ECRIS-TCN system], and the European search portal <i>ESP</i> , the shared biometric matching service <i>BMS</i> , the common identity repository <i>CIR</i> , <i>the MID</i> and the multiple-identity detector <i>CRRS</i> .	3. eu-LISA shall be responsible for the development of the interoperability components, for any adaptations required for establishing interoperability between the central systems of the EES, VIS, [ETIAS], SIS, and Eurodac, and [the ECRIS-TCN system], and the European search portal (<i>ESP</i>), the shared biometric matching service (<i>BMS</i>), the common identity repository (<i>CIR</i>), and the multiple-identity detector (<i>MID</i>) <i>and the central repository for reporting and statistics (CRRS)</i> .	
619	eu-LISA shall define the design of the physical architecture of the interoperability components including their communication infrastructures and the technical specifications and their evolution as regards the central infrastructure and the secure communication infrastructure, which shall be adopted by the	eu-LISA shall define the design of the physical architecture of the interoperability components including their communication infrastructures and the technical specifications and their evolution as regards the central infrastructure and the secure communication infrastructure, which shall be adopted by the	eu-LISA shall define the design of the physical architecture of the interoperability components including their communication infrastructures and the technical specifications and their evolution as regards the central infrastructure and the secure communication infrastructure, which shall be adopted by the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the EES, [ETIAS], SIS or VIS deriving from the establishment of interoperability and provided for by this Regulation.	Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the EES, [ETIAS], SIS or VIS deriving from the establishment of interoperability and provided for by this Regulation.	Management Board, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the EES, VIS , [ETIAS]; or SIS or VIS deriving from the establishment of interoperability and provided for by this Regulation.	
620	eu-LISA shall develop and implement the interoperability components as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5).	eu-LISA shall develop and implement the interoperability components as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5).	eu-LISA shall develop and implement the interoperability components as soon as possible after the entry into force of this Regulation and the adoption by the Commission of the measures provided for in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5), and 44(5) and 68(7a) .	
621	The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project coordination.	The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project management and coordination. eu-LISA shall follow the principles of privacy by design and by default during the entire lifecycle of the	The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project coordination.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>development of the interoperability components.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
622	<p>4. During the design and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or its alternates, the Chair of the Interoperability Advisory Group referred to in Article 65, a member representing eu-LISA appointed by its Executive Director, and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States that are fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA and which will participate in the interoperability components.</p>	<p>4. During the design and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or its alternates, the Chair of the Interoperability Advisory Group referred to in Article 65, a member representing eu-LISA appointed by its Executive Director, and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States that are fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA and which will participate in the interoperability components.</p>	<p>4. During the design and development phase, a Programme Management Board composed of a maximum of 10 members shall be established. It shall be composed of seven members appointed by eu-LISA's Management Board from among its members or its alternates, the Chair of the Interoperability Advisory Group referred to in Article 65, a member representing eu-LISA appointed by its Executive Director, and one member appointed by the Commission. The members appointed by eu-LISA's Management Board shall be elected only from those Member States that are fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT EU information systems managed by eu-LISA and which will participate in the interoperability components.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
623	5. The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of the interoperability components.	5. The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of the interoperability components.	5. The Programme Management Board shall meet regularly and at least three times per quarter. It shall ensure the adequate management of the design and development phase of the interoperability components.	
624	The Programme Management Board shall every month submit to the Management Board written reports on progress of the project. The Programme Management Board shall have no decision-making power nor any mandate to represent the members of eu-LISA's Management Board.	The Programme Management Board shall every month submit to the Management Board written reports on progress of the project. The Programme Management Board shall have no decision-making power nor any mandate to represent the members of eu-LISA's Management Board.	The Programme Management Board shall every month submit to <i>eu-LISA's</i> the Management Board written reports on progress of the project. The Programme Management Board shall have no decision-making power nor any mandate to represent the members of eu-LISA's Management Board.	
625	6. eu-LISA's Management Board shall establish the rules of procedure of the Programme Management Board, which shall include in particular rules on:	6. eu-LISA's Management Board shall establish the rules of procedure of the Programme Management Board, which shall include in particular rules on:	6. eu-LISA's Management Board shall establish the rules of procedure of the Programme Management Board, which shall include in particular rules on:	
626	(a) chairmanship;	(a) chairmanship;	(a) chairmanship;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
627	(b) meeting venues;	(b) meeting venues;	(b) meeting venues;	
628	(c) preparation of meetings;	(c) preparation of meetings;	(c) preparation of meetings;	
629	(d) admission of experts to the meetings;	(d) admission of experts to the meetings;	(d) admission of experts to the meetings;	
630	(e) communication plans ensuring full information to non-participating Members of the Management Board.	(e) communication plans ensuring full information to non-participating Members of the Management Board.	(e) communication plans ensuring full information to non-participating Members of the Management Board.	
631	The chairmanship shall be held by a Member State that is fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA.	The chairmanship shall be held by a Member State that is fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the large-scale IT systems managed by eu-LISA.	The chairmanship shall be held by a Member State that is fully bound under Union law by the legislative instruments governing the development, establishment, operation and use of all the <i>EU information systems</i> large-scale IT systems managed by eu-LISA.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
632	All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by the Agency, and Article 10 of the eu-LISA Rules of Procedure shall apply <i>mutatis mutandis</i> . eu-LISA shall provide the Programme Management Board with a secretariat.	All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by the Agency, and Article 10 of the eu-LISA Rules of Procedure shall apply <i>mutatis mutandis</i> . eu-LISA shall provide the Programme Management Board with a secretariat.	All travel and subsistence expenses incurred by the members of the Programme Management Board shall be paid by the Agency, and Article 10 of the eu-LISA Rules of Procedure shall apply <i>mutatis mutandis</i> . eu-LISA shall provide the Programme Management Board with a secretariat.	
633	The Interoperability Advisory Group referred to in Article 65 shall meet regularly until the start of operations of the interoperability components. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.	The Interoperability Advisory Group referred to in Article 65 shall meet regularly until the start of operations of the interoperability components. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.	The Interoperability Advisory Group referred to in Article 65 shall meet regularly until the start of operations of the interoperability components. It shall report after each meeting to the Programme Management Board. It shall provide the technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
634	<i>Article 53 Responsibilities of eu-LISA following the entry into operations</i>	<i>Article 53 Responsibilities of eu-LISA following the entry into operations</i>	<i>Article 53 Responsibilities of eu-LISA following the entry into operations</i>	
635	1. Following the entry into operations of each interoperability component, eu-LISA shall be responsible for the technical management of the central infrastructure and the national uniform interfaces. In cooperation with the Member States, it shall ensure at all times the best available technology, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the communication infrastructure referred to in Articles 6, 12, 17, 25 and 39.	Following the entry into operations of each interoperability component, eu-LISA shall be responsible for the technical and security management of the central infrastructure and the national uniform interfaces of the interoperability components, including maintenance and technological developments . In cooperation with the Member States, it shall ensure that at all times the best available technology is used , subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management and security of the communication infrastructure referred to in Articles 6, 12, 17, 25 and 39.	1. Following the entry into operations of each interoperability component, eu-LISA shall be responsible for the technical management of the central infrastructure and the national uniform interfaces . In cooperation with the Member States, it shall ensure at all times the best available technology, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the communication infrastructure referred to in Articles 6, 12, 17, 25 and 39.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
636	Technical management of the interoperability components shall consist of all the tasks necessary to keep the interoperability components 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 components function at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central infrastructures in accordance with the technical specifications.	Technical management of the interoperability components shall consist consists of all the tasks necessary to keep the interoperability components 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 components function at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central infrastructures in accordance with the technical specifications.	Technical management of the interoperability components shall consist of all the tasks necessary to keep the interoperability components functioning <i>providing uninterrupted services to the Member States</i> 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 components function at a satisfactory level of technical quality, in particular as regards the response time for interrogation of the central infrastructures in accordance with the technical specifications.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
637		<i>Security management of the interoperability components shall consist of all the tasks necessary to ensure the integrity, confidentiality and availability of all interoperability components in accordance with this Regulation, in particular information security risk assessments and preventive measures to avoid both physical and IT security incidents and the actions required to respond and recover from them if they cannot be avoided.</i>		
638	2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its entire staff required to work with data stored in the interoperability components. This obligation shall also apply after such staff leave	2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its entire staff required to work with data stored in the interoperability components. This obligation shall also apply after such staff leave	2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its entire staff required to work with data stored in the interoperability components. This obligation shall also apply after such staff leave	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	office or employment or after the termination of their activities.	office or employment or after the termination of their activities.	office or employment or after the termination of their activities.	
639	3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared biometric matching service and the common identity repository in accordance with Article 37.	3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared biometric matching service and the common identity repository in accordance with Article 37.	3. eu-LISA shall develop and maintain a mechanism and procedures for carrying out quality checks on the data stored in the shared biometric matching service and the common identity repository in accordance with Article 37.	
640	4. eu-LISA shall also perform tasks related to providing training on the technical use of the interoperability components.	4. eu-LISA shall also perform tasks related to providing training on the technical use of the interoperability components.	4. eu-LISA shall also perform tasks related to providing training on the technical use of the interoperability components.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
641	<i>Article 54 Responsibilities of Member States</i>	<i>Article 54 Responsibilities of Member States</i>	<i>Article 54 Responsibilities of Member States</i>	
642	1. Each Member State shall be responsible for:	1. Each Member State shall be responsible for:	1. Each Member State shall be responsible for:	
643	(a) the connection to the communication infrastructure of the European search portal (ESP) and the common identity repository (CIR);	(a) the connection to the communication infrastructure of the European search portal (ESP) and the common identity repository (CIR);	(a) the connection to the communication infrastructure of the European search portal (ESP) and the common identity repository (CIR) ;	
644	(b) the integration of the existing national systems and infrastructures with the ESP, shared biometric matching service, the CIR and the multiple-identity detector;	(b) the integration of the existing national systems and infrastructures with the ESP, shared biometric matching service, the CIR and the multiple-identity detector;	(b) the integration of the existing national systems and infrastructures with the ESP, shared biometric matching service , the CIR and the multiple-identity detector MID ;	
645	(c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the interoperability components;	(c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the interoperability components;	(c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the interoperability components;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
646	(d) the management of, and arrangements for, access by the duly authorised staff, and by the duly empowered staff, of the competent national authorities to the ESP, the CIR and the multiple-identity detector in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;	(d) the management of, and arrangements for, access by the duly authorised staff, and by the duly empowered staff, of the competent national authorities to the ESP, the CIR and the multiple-identity detector in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;	(d) the management of, and arrangements for, access by the duly authorised staff and by the duly empowered staff of the competent national authorities to the ESP, the CIR and the multiple-identity detector MID in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;	
647	(e) the adoption of the legislative measures referred to in Article 20(3) in order to access the CIR for identification purposes;	(e) the adoption of the legislative measures referred to in Article 20(3) in order to access the CIR for identification purposes;	(e) the adoption of the legislative measures referred to in Article 20 (3) (2) and 20(2a) in order to access the CIR for identification purposes;	
648	(f) the manual verification of different identities referred to in Article 29;	(f) the manual verification of different identities referred to in Article 29;	(f) the manual verification of different identities referred to in Article 29;	
649	(g) the implementation of data quality requirements in the EU information systems and in the interoperability components;	(g) the implementation of data quality requirements in the EU information systems and in the interoperability components;	(g) the implementation compliance with data quality requirements in the EU information systems and in the interoperability components established under Union law ;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
650		<i>(ga) fully complying with the rules of each IT system to ensure the security and integrity of personal data;</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
651	(h) remedying any deficiencies identified in the Commission's evaluation report concerning data quality referred to in Article 37(5).	(h) remedying any deficiencies identified in the Commission's evaluation report concerning data quality referred to in Article 37(5).	(h) remedying any deficiencies identified in the Commission's evaluation report concerning data quality referred to in Article 37(5).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
652		<i>(ha) reporting any security incidents involving personal data to the Commission, eu-LISA, the national supervisory authorities and the European Data Protection Supervisor.</i>		
653	2. Each Member State shall connect their designated authorities referred to in Article 4(24) to the CIR.	2. Each Member State shall connect their designated authorities referred to in Article 4(24) to the CIR.	2. Each Member State shall connect their designated authorities referred to in Article 4(24) to the CIR.	
654		Article 54a Responsibilities of Europol		
655		<i>1. Europol shall ensure processing of the queries by the ESP and the shared BMS to Europol data and shall accordingly adapt its Querying Europol Systems (QUEST) interface for basic protection level (BPL) data.</i>		
656		<i>2. Europol shall be responsible for the management of, and arrangements for, its duly authorised staff to use and access respectively the ESP and</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>the CIR in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles.</i>		
657		3. Any data processing by Europol under this Regulation shall be subject to Regulation (EU) 2016/794.		
658	<i>Article 55 Responsibilities of the ETIAS Central Unit</i>	<i>Article 55 Responsibilities of the ETIAS Central Unit</i>	<i>Article 55 Responsibilities of the ETIAS Central Unit</i>	
659	The ETIAS Central Unit shall be responsible for:	The ETIAS Central Unit shall be responsible for:	The ETIAS Central Unit shall be responsible for:	
660	(a) the manual verification of different identities referred to in Article 29;	(a) the manual verification of different identities referred to in Article 29;	(a) the manual verification of different identities referred to in Article 29;	
661	(b) carrying out a multiple-identity detection between the data stored in the VIS, Eurodac and the SIS referred to in Article 59.	(b) carrying out a multiple-identity detection between the data stored in the VIS, Eurodac and the SIS referred to in Article 59.	(b) carrying out a multiple-identity detection between the data stored in the EES , VIS, Eurodac and the SIS referred to in Article 59.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
662	CHAPTER IX Amendments to other Union instruments	CHAPTER IX Amendments to other Union instruments	CHAPTER IX Amendments to other Union instruments	
663	<i>Article 55a Amendments to Regulation (EU) 2016/399</i>	<i>Article 55a Amendments to Regulation (EU) 2016/399</i>	<i>Article 55a Amendments to Regulation (EU) 2016/399</i>	
664	Regulation (EU) 2016/399 is amended as follows:	Regulation (EU) 2016/399 is amended as follows:	Regulation (EU) 2016/399 is amended as follows:	
665	In Article 8 of Regulation (EU) 2016/399, the following paragraph 4a is added:	In Article 8 of Regulation (EU) 2016/399, the following paragraph 4a is added:	In Article 8 of Regulation (EU) 2016/399, the following paragraph 4a is added:	
666	"4a. The border guard at second line shall consult the multiple-identity detector together with the common identity repository referred to in [Article 4(35) of Regulation 2018/XX on interoperability] or the Schengen Information System or both to assess the differences in the linked identities and shall carry out any additional verification necessary to take a decision on the status and colour of the link	The border guard at second line shall consult the multiple-identity detector together with the common identity repository referred to in [Article 4(35) of Regulation 2018/XX on interoperability] or the Schengen Information System or both to assess the differences in the linked identities and shall carry out any additional verification necessary to take a decision on the status and colour of the link	"4a. The border guard at second line shall consult the multiple-identity detector together with the common identity repository referred to in [Article 4(35) of Regulation 2018/XX on interoperability] or the Schengen Information System or both to assess the differences in the linked identities <i>data and travel document data</i> , and shall carry out any additional verification necessary to take a decision on	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	as well as to take a decision on the entry or refusal of entry of the person concerned.	as well as to take a decision on the entry or refusal of entry of the person concerned.	the status and colour of the link as well as to take a decision on the entry or refusal of entry of the person concerned.	
667	In accordance with [Article 59(1) of Regulation 2018/XX], this paragraph shall apply only as from the start of operations of the multiple-identity detector."	In accordance with [Article 59(1) of Regulation 2018/XX], this paragraph shall apply only as from the start of operations of the multiple-identity detector."	In accordance with [Article 59(1) of Regulation 2018/XX], this paragraph shall apply only as from the start of operations of the multiple-identity detector."	
668	<i>Article 55b Amendments to Regulation (EU) 2017/2226</i>	<i>Article 55b Amendments to Regulation (EU) 2017/2226</i>	<i>Article 55b Amendments to Regulation (EU) 2017/2226</i>	
669	Regulation (EU) 2017/2226 is amended as follows:	Regulation (EU) 2017/2226 is amended as follows:	Regulation (EU) 2017/2226 is amended as follows:	
670	1) In Article 1, the following paragraph is added:	1) In Article 1, the following paragraph is added:	1) In Article 1, the following paragraph is added:	
671	"1a. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the EES contributes to facilitating and assisting in the correct identification of persons	"1a. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the EES contributes to facilitating and assisting in the correct identification of persons	"1a. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the EES contributes to facilitating and assisting in the correct identification of persons	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	registered in the EES under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."	registered in the EES under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."	registered in the EES under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."	
672	2) In Article 3, the following point (21a) is added:	2) In Article 3, the following point (21a) is added:	2) In Article 3, the following point (21a) is added:	
673	"'CIR' means the common identity repository as defined in [Article 4(35) of Regulation 2018/XX on interoperability]	"'CIR' means the common identity repository as defined in [Article 4(35) of Regulation 2018/XX on interoperability]	"'CIR' means the common identity repository as defined in [Article 4(35) of Regulation 2018/XX on interoperability]	
674	3) Article 3(1)(22) shall be replaced by the following:	3) Article 3(1)(22) shall be replaced by the following:	3) Article 3(1)(22) shall be replaced by the following:	
675	"(22) 'EES data' means all data stored in the EES Central System and in the CIR in accordance with Article 14 and Articles 16 to 20.	"(22) 'EES data' means all data stored in the EES Central System and in the CIR in accordance with Article 14 and Articles 16 to 20.	"(22) 'EES data' means all data stored in the EES Central System and in the CIR in accordance with Article 14 and Articles 15 16 to 20.	
676	4) In Article 3, a new point (22a) is added:	4) In Article 3, a new point (22a) is added:	4) In Article 3, a new point (22a) is added:	
677	"(22a) 'identity data' means the data referred to in Article 16(1)(a);	"(22a) 'identity data' means the data referred to in Article 16(1)(a);	"(22a) 'identity data' means the data referred to in Article 16(1)(a), <i>as well the relevant data referred to in Articles 17(1) and 18(1)</i> ;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
678	5) In Article 6(1), the following point is inserted:	5) In Article 6(1), the following point is inserted:	5) In Article 6(1), the following point is inserted:	
679	"(j) ensure the correct identification of persons."	"(j) ensure the correct identification of persons."	"(j) ensure the correct identification of persons."	
680	6) Article 7(1)(a) is replaced by the following:	6) Article 7(1)(a) is replaced by the following:	6) Article 7(1)(a) is replaced by the following:	
681	"(a) the common identity repository (CIR) as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability];	"(a) the common identity repository (CIR) as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability];	"(a) the common identity repository (CIR) as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability];	
682	(aa) a Central System (EES Central System);"	(aa) a Central System (EES Central System);"	(aa) a Central System (EES Central System);"	
683	7) In Article 7(1), point (f) is replaced by the following:	7) In Article 7(1), point (f) is replaced by the following:	7) In Article 7(1), point (f) is replaced by the following:	
684	"(f) a secure communication infrastructure between the EES Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], the shared biometric matching service established by [Article 12 of Regulation 2018/XX on	"(f) a secure communication infrastructure between the EES Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], the shared biometric matching service established by [Article 12 of Regulation 2018/XX on	"(f) a secure communication infrastructure between the EES Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], the shared biometric matching service established by [Article 12 of Regulation 2018/XX on	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	interoperability], the common identity repository established by [Article 17 of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability]".	interoperability], the common identity repository established by [Article 17 of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability]".	interoperability] , and the common identity repository established by [Article 17(1) of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability] ".	
685	8) In Article 7, the following paragraph is added:	8) In Article 7, the following paragraph is added:	8) In Article 7, the following paragraph is added:	
686	"1a. The CIR shall contain the data referred to in Article 16(1)(a) to (d) and Article 17(1)(a) to (c), the remaining EES data shall be stored in the EES Central System.	"1a. The CIR shall contain the data referred to in Article 16(1)(a) to (d) and Article 17(1)(a) to (c), the remaining EES data shall be stored in the EES Central System.	"1a. The CIR shall contain the data referred to in Article 16(1)(a) to (d), and Article 17(1)(a) to (c) and Article 18(1) and (2) , the remaining EES data shall be stored in the EES Central System.	
687	9) In Article 9, the following paragraph is added:	9) In Article 9, the following paragraph is added:	9) In Article 9, the following paragraph is added:	
688	"3. Access to consulting the EES data stored in the CIR shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the EU bodies that are	"3. Access to consulting the EES data stored in the CIR shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the EU bodies that are	"3. 4. Access to consulting the EES data stored in the CIR shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the EU	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and EU bodies in accordance with those purposes and shall be proportionate to the objectives pursued."	competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and EU bodies in accordance with those purposes and shall be proportionate to the objectives pursued."	<i>agencies</i> bodies that are competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and EU <i>agencies</i> bodies in accordance with those purposes and shall be proportionate to the objectives pursued."	
689	10) In Article 21(1), the words "EES Central System" are replaced, both times they appear, by the words "EES Central System or the CIR".	10) In Article 21(1), the words "EES Central System" are replaced, both times they appear, by the words "EES Central System or the CIR".	10) In Article 21(1), the words "EES Central System" are replaced, both times <i>every time</i> they appear, by the words "EES Central System or the CIR".	
690	11) In Article 21(2), the words "both the EES Central System and in the NUI" are replaced by the words "both the EES Central System and the CIR on the one hand and in the NUI on the other".	11) In Article 21(2), the words "both the EES Central System and in the NUI" are replaced by the words "both the EES Central System and the CIR on the one hand and in the NUI on the other".	11) In Article 21(2), the words "both the EES Central System and in the NUI" are replaced by the words "both the EES Central System and the CIR on the one hand and in the NUI on the other".	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
691	12) In Article 21(2), the words "shall be entered in the EES Central System" are replaced by the words "shall be entered in the EES Central System and the CIR".	12) In Article 21(2), the words "shall be entered in the EES Central System" are replaced by the words "shall be entered in the EES Central System and the CIR".	12) In Article 21(2), the words "shall be entered in the EES Central System" are replaced by the words "shall be entered in the EES Central System and the CIR".	
692			<i>12a) A new paragraph 2a is added to Article 23:</i>	
693			<i>"2a. For the purpose of the verifications set out in paragraph 1, the border authority shall launch a query by using the European Search Portal defined in [Article 6(1) of the Interoperability Regulation] to compare the data on the third-country national with the relevant data of the EES and the VIS."</i>	
694			<i>12b) Article 23(4) is replaced by the following:</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
695			<i>"4. Where the search with the alphanumeric data set out in paragraph 2 of this Article indicates that data on the third-country national are not recorded in the EES, where a verification of the third-country national pursuant to paragraph 2 of this Article fails or where there are doubts as to the identity of the third-country national, the border authorities shall have access to data for identification in accordance with Article 27 of this Regulation in order to create or update an individual file in accordance with Article 14.</i>	
696			<i>In addition to the identification referred to in first subparagraph of this paragraph, the following provisions shall apply:</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
697			<p><i>(a) for third-country nationals who are subject to a visa requirement, if the search in the VIS with the data referred to in Article 18(1) of Regulation (EC) No 767/2008 indicates that data on the third-country national are recorded in the VIS, a verification of fingerprints against the VIS shall be carried out in accordance with Article 18(5) of Regulation (EC) No 767/2008. For this purpose, the border authority may launch a search from the EES to the VIS as provided for in Article 18(6) of Regulation (EC) No 767/2008. Where a verification of a third-country national pursuant to paragraph 2 of this Article failed, the border authorities shall access the VIS data for identification in accordance with Article 20 of Regulation (EC) No 767/2008.</i></p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
698			<i>(b) for third-country nationals who are not subject to a visa requirement and for whom no data are found in the EES further to the identification run in accordance with Article 27 of this Regulation, the VIS shall be consulted in accordance with Article 19a of Regulation (EC) No 767/2008. The border authority may launch a search from the EES to the VIS as provided for in Article 19a of Regulation (EC) No 767/2008."</i>	
699	13) A new paragraph (1a) is added to Article 32:	13) A new paragraph (1a) is added to Article 32:	13) A new paragraph (1a) is added to Article 32:	
700	"1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the EES."	1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation <i>where the conditions laid down in this Article are met and</i> where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on	"1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data <i>are</i> is stored in the EES."	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		interoperability] reveals that data is stored in the EES.		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
701	14) Article 32(2) is replaced by the following:	14) Article 32(2) is replaced by the following:	14) Article 32(2) is replaced by the following:	
702	"2. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or otherwise serious criminal offence shall only be allowed when a query to the CIR was launched in accordance with [Article 22 of Regulation 2018/XX on interoperability] and all the conditions listed in paragraph 1 and paragraph 1a are met.	Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or otherwise offence or other serious criminal offence shall only be allowed when a query to the CIR was launched in accordance with [Article 22 of Regulation 2018/XX on interoperability] and all the conditions listed in paragraph 1 and paragraph 1a of this Article are met.	"2. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence offence or otherwise serious criminal offence shall only be allowed when a query to the CIR was launched in accordance with [Article 22 of Regulation 2018/XX on interoperability] and all the conditions listed in paragraph 1 and paragraph 1a are met.	
703	However, this additional condition shall not apply in a case of urgency where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request sent by the operating unit of the designated	However, this additional condition shall not apply in a case of urgency where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request sent by the operating unit of the designated	However, this additional condition shall not apply in a case of urgency where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence. Those reasonable grounds shall be included in the electronic or written request sent by the operating unit of the designated	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	authority to the central access point."	authority to the central access point."	authority to the central access point."	
704	15) Article 32(4) is deleted.	15) Article 32(4) is deleted.	15) Article 32(4) is deleted.	
705	16) A new paragraph (1a) is added to Article 33:	16) A new paragraph (1a) is added to Article 33:	16) A new paragraph (1a) is added to Article 33:	
706	"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the EES."	1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation <i>where the conditions laid down in this Article are met and</i> where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the EES.	"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access EES for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data <i>are</i> is stored in the EES."	
707			<i>16a) Article 33(2), subparagraph 2 is deleted.</i>	
708	17) In Article 33, paragraph 3 is replaced by the following:	17) In Article 33, paragraph 3 is replaced by the following:	17) In Article 33, paragraph 3 is replaced by the following:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
709	"The conditions laid down in Article 32(3) and (5) shall apply accordingly"	"The conditions laid down in Article 32(3) and (5) shall apply accordingly"	"The conditions laid down in Article 32(3) and (5) shall apply accordingly".	
710	18) In Article 34(1) and (2), the words "in the EES Central System" shall be replaced by the words "in the CIR and in the EES Central System respectively".	18) In Article 34(1) and (2), the words "in the EES Central System" shall be replaced by the words "in the CIR and in the EES Central System respectively".	18) In Article 34(1) and (2), the words "in the EES Central System" shall be replaced by the words "in the CIR and in the EES Central System respectively".	
711			<i>18a) In Article 34, a new paragraph 3a is added:</i>	
712			<i>"3a. Where a red link is stored in the multiple identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability] in accordance with [Article 32 of Regulation 2018/XX on interoperability], the linked EES data referred to in Article 16(1)(a) to (d) and Article 17(1)(a) to (c) and Article 18(1) and (2) shall be stored in the CIR in accordance with [Article 23(3) of Regulation 2018/XX on interoperability]."</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
713	19) In Article 34(5), the words "of the EES Central System" shall be replaced by the words "from the EES Central System and from the CIR".	19) In Article 34(5), the words "of the EES Central System" shall be replaced by the words "from the EES Central System and from the CIR".	19) In Article 34(5), the words "of the EES Central System" shall be replaced by the words "from the EES Central System and from the CIR".	
714	20) In Article 35, paragraph 7 is replaced by the following:	20) In Article 35, paragraph 7 is replaced by the following:	20) In Article 35, paragraph 7 is replaced by the following:	
715	"The EES Central System and the CIR shall immediately inform all Member States of the erasure of EES or CIR data and where applicable remove them from the list of identified persons referred to in Article 12(3)."	"The EES Central System and the CIR shall immediately inform all Member States of the erasure of EES or CIR data and where applicable remove them from the list of identified persons referred to in Article 12(3)."	"The EES Central System and the CIR shall immediately inform all Member States of the erasure of EES or CIR data and where applicable remove them from the list of identified persons referred to in Article 12(3)."	
716	21) In Article 36, the words "of the EES Central System" shall be replaced by the words "of the EES Central System and the CIR".	21) In Article 36, the words "of the EES Central System" shall be replaced by the words "of the EES Central System and the CIR".	21) In Article 36, the words "of the EES Central System" shall be replaced by the words "of the EES Central System and the CIR".	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
717	22) In Article 37(1), the words "development of the EES Central System", shall be replaced by the words "development of the EES Central System and the CIR".	22) In Article 37(1), the words "development of the EES Central System", shall be replaced by the words "development of the EES Central System and the CIR".	22) In Article 37(1), the words "development of the EES Central System", shall be replaced by the words "development of the EES Central System and the CIR".	
718	23) In the first subparagraph of Article 37(3), the words "the EES Central System" shall be replaced, the first and the third time they appear, by the words "the EES Central System and the CIR".	23) In the first subparagraph of Article 37(3), the words "the EES Central System" shall be replaced, the first and the third time they appear, by the words "the EES Central System and the CIR".	23) In the first subparagraph of Article 37(3), the words "the EES Central System" shall be replaced, the first and the third time they appear, by the words "the EES Central System and the CIR".	
719	24) In Article 46(1) the following point (f) is added:	24) In Article 46(1) the following point (f) is added:	24) In Article 46(1) the following point (f) is added:	
720	"(f) where relevant, a reference to the use of the European search portal to query the EES as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability]."	"(f) where relevant, a reference to the use of the European search portal to query the EES as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability]."	"(f) where relevant , a reference to the use of the European search portal to query the EES as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability]."	
721		<i>(24a) In Article 52, the following paragraph is added:</i>		
722		<i>7a. Third-country nationals wishing to exercise their rights</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<p><i>under this Article may make use of the web service as provided for in Article 47 of [the Regulation on establishing a framework for interoperability between Union information systems (border and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU)2016/399, Regulation (EU) 2017/2226], Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation].</i></p>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
723	25) Article 63(2) is replaced by the following:	25) Article 63(2) is replaced by the following:	25) Article 63(2) is replaced by the following:	
724	"2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]."	"2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]."	"2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]."	
725	26) In Article 63(4) a new subparagraph is added:	26) In Article 63(4) a new subparagraph is added:	26) In Article 63(4) a new subparagraph is added:	
726	"The daily statistics shall be stored in the central repository for reporting and statistics."	"The daily statistics shall be stored in the central repository for reporting and statistics."	"The daily statistics shall be stored in the central repository for reporting and statistics."	
727	<i>Article 55c</i>	<i>Article 55c</i>	<i>Article 55c</i>	
728	<i>Amendments to Council Decision 2004/512/EC</i>	<i>Amendments to Council Decision 2004/512/EC</i>	<i>Amendments to Council Decision 2004/512/EC</i>	
729	Council Decision 2004/512/EC establishing the Visa Information System (VIS) is amended as follows:	Council Decision 2004/512/EC establishing the Visa Information System (VIS) is amended as follows:	Council Decision 2004/512/EC establishing the Visa Information System (VIS) is amended as follows:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
730	Article 1(2) is amended as follows:	Article 1(2) is amended as follows:	Article 1(2) is amended as follows:	
731	"2. The Visa Information System shall be based on a centralised architecture and consist of:	"2. The Visa Information System shall be based on a centralised architecture and consist of:	"2. The Visa Information System shall be based on a centralised architecture and consist of:	
732	a) the common identity repository as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability],	a) the common identity repository as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability],	a) the common identity repository as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability],	
733	b) a central information system, hereinafter referred to as ‘the Central Visa Information System’ (CS-VIS),	b) a central information system, hereinafter referred to as ‘the Central Visa Information System’ (CS-VIS),	b) a central information system, hereinafter referred to as ‘the Central Visa Information System’ (CS-VIS),	
734	c) an interface in each Member State, hereinafter referred to as ‘the National Interface’ (NI-VIS) which shall provide the connection to the relevant central national authority of the respective Member State;	c) an interface in each Member State, hereinafter referred to as ‘the National Interface’ (NI-VIS) which shall provide the connection to the relevant central national authority of the respective Member State;	c) an interface in each Member State, hereinafter referred to as ‘the National Interface’ (NI-VIS) which shall provide the connection to the relevant central national authority of the respective Member State;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
735	d) a communication infrastructure between the Central Visa Information System and the National Interfaces;	d) a communication infrastructure between the Central Visa Information System and the National Interfaces;	d) a communication infrastructure between the Central Visa Information System and the National Interfaces;	
736	e) a Secure Communication Channel between the EES Central System and the CS-VIS;	e) a Secure Communication Channel between the EES Central System and the CS-VIS;	e) a Secure Communication Channel between the EES Central System and the CS-VIS;	
737	f) a secure communication infrastructure between the VIS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], shared biometric matching service established by [Article 12 of Regulation 2018/XX on interoperability], the common identity repository and the multiple-identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability]".	f) a secure communication infrastructure between the VIS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], shared biometric matching service established by [Article 12 of Regulation 2018/XX on interoperability], the common identity repository and the multiple-identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability]".	f) a secure communication infrastructure between the VIS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], shared biometric matching service established by [Article 12 of Regulation 2018/XX on interoperability] , and the common identity repository and the multiple-identity detector (MID) established by [Article 17(I) 25 of Regulation 2018/XX on interoperability]".	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
738	<i>Article 55d</i> <i>Amendments to Regulation (EC) 767/2008</i>	<i>Article 55d</i> <i>Amendments to Regulation (EC) 767/2008</i>	<i>Article 55d</i> <i>Amendments to Regulation (EC) 767/2008</i>	
739	1) In Article 1, the following paragraph is added:	(1) In Article 1 2, the following paragraph is added:	1) In Article 1, the following paragraph is added:	
740	"2. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS under the conditions and for the ultimate objectives laid down in paragraph 1 of this Article."	2. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS under the conditions and <i>solely</i> for the ultimate objectives laid down in paragraph 1 of this Article <i>purpose of identification referred to in Article 20 of this Regulation.</i>	"2. By storing identity, travel document and biometric data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the VIS contributes to facilitating and assisting in the correct identification of persons registered in the VIS under the conditions and for the ultimate objectives laid down in paragraph 1 of this Article <i>referred to in [Article 20] of that Regulation.</i> "	
741	2) In Article 4, the following points are added:	2) In Article 4, the following points are added:	2) In Article 4, the following points are added:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
742	"(12) 'VIS data' means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to14.	"(12) 'VIS data' means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to14.	"(12) 'VIS data' means all data stored in the VIS Central System and in the CIR in accordance with Articles 9 to14.	
743	"(13) 'identity data' means the data referred to in Article 9(4)(a) to aa);	"(13) 'identity data' means the data referred to in Article 9(4)(a) to aa);	"(13) 'identity data' means the data referred to in Article 9(4)(a) to aa);	
744	(14) 'fingerprint data' means the data relating to the five fingerprints of the index, middle finger, ring finger, little finger and the thumb from the right hand where present, and from the left hand;	(14) 'fingerprint data' means the data relating to the five fingerprints of the index, middle finger, ring finger, little finger and the thumb from the right hand where present, and from the left hand;	(14) 'fingerprint data' means the data relating to the five fingerprints of the index, middle finger, ring finger, little finger and the thumb from the right hand where present, and from the left hand;	
745	(15) 'facial image' means digital images of the face;	(15) 'facial image' means digital images of the face;	(15) 'facial image' means digital images of the face;	
746	(16) 'biometric data' means fingerprint data and facial image;"	(16) 'biometric data' means fingerprint data and facial image;"	(16) 'biometric data' means fingerprint data and facial image;"	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
747	3) In Article 5, the following paragraph is added:	3) In Article 5, the following paragraph is added:	3) In Article 5, the following paragraph is added:	
748	"1a). The CIR shall contain the data referred to in Article 9(4)(a) to (cc), 9(5) and 9(6), the remaining VIS data shall be stored in the VIS Central System."	"1a). The CIR shall contain the data referred to in Article 9(4)(a) to (cc), 9(5) and 9(6), the remaining VIS data shall be stored in the VIS Central System."	"1a). The CIR shall contain the data referred to in Article 9(4)(a) to (ce), 9(5) and 9(6), the remaining VIS data shall be stored in the VIS Central System."	
749	4) Article 6(2) is amended as follows:	4) Article 6(2) is amended as follows:	4) Article 6(2) is amended as follows:	
750	"2. Access to the VIS for consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Article 15 to 22, and for the duly authorised staff of the national authorities of each Member State and of the EU bodies which are competent for the purposes laid down in [Article 20 and Article 21 of the Regulation 2018/XX on interoperability], limited to the extent that the data are required	"2. Access to the VIS for consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Article 15 to 22, and for the duly authorised staff of the national authorities of each Member State and of the EU bodies which are competent for the purposes laid down in [Article 20 and Article 21 of the Regulation 2018/XX on interoperability], limited to the extent that the data are required	"2. Access to the VIS for consulting the data shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Article 15 to 22, and for the duly authorised staff of the national authorities of each Member State and of the EU bodies agencies which are competent for the purposes laid down in [Article 20 and Article 21 of the Regulation 2018/XX on interoperability], limited to the extent that the data are required	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued."	for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued."	for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued."	
751	5) Article 9(4) (a) to (c) is amended as follows:	5) Article 9(4) (a) to (c) is amended as follows:	5) Article 9(4) (a) to (c) is amended as follows:	
752	"(a) surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex;	"(a) surname (family name); first name or names (given names); date of birth; nationality or nationalities; sex;	"(a) surname (family name); first name or names (given names); date of birth; nationality or nationalities ; sex;	
753	(aa) surname at birth (former surname(s)); place and country of birth; nationality at birth;	(aa) surname at birth (former surname(s)); place and country of birth; nationality at birth;	(aa) surname at birth (former surname(s)); place and country of birth; current nationality and nationality at birth;	
754	(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;	(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;	(b) the type and number of the travel document or documents and the three-letter code of the issuing country of the travel document or documents;	
755	(c) the date of expiry of the validity of the travel document or documents;	(c) the date of expiry of the validity of the travel document or documents;	(c) the date of expiry of the validity of the travel document or documents;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
756	(cc) the authority which issued the travel document and its date of issue;	(cc) the authority which issued the travel document and its date of issue;	(cc) the authority which issued the travel document and its date of issue;	
757	6) Article 9(5) is replaced by the following:	6) Article 9(5) is replaced by the following:	6) Article 9(5) is replaced by the following:	
758	"facial image as defined in Article 4(15)".	"facial image as defined in Article 4(15)".	"facial image as defined in Article 4(15)".	
759			<i>6a) A second sentence is added in Article 23(1), as follows:</i>	
760			<i>"Where a red link is stored in the multiple identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability] in accordance with [Article 32 of Regulation 2018/XX on interoperability], the linked VIS data referred to in Article 9(4)(a) to (cc), 9(5) and 9(6) shall be stored in the CIR in accordance with [Article 23(3) of Regulation 2018/XX on interoperability]"</i> .	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
761	7) In Article 29(2)(a) the word "VIS" is replaced by the words "VIS or the CIR" in both instances where it appears.	7) In Article 29(2)(a) the word "VIS" is replaced by the words "VIS or the CIR" in both instances where it appears.	7) In Article 29(2)(a) the word "VIS" is replaced by the words "VIS or the CIR" in both instances where it appears.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
762		<i>(7a) In Article 38, the following paragraph is added:</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
763		<i>6a. Third-country nationals wishing to exercise their rights under this Article may make use of the web service provided for in Article 47 of [Regulation on establishing a framework for interoperability between Union information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation].</i>		
764	<i>Article 55e Amendments to Council Decision 2008/633/JHA</i>	<i>Article 55e Amendments to Council Decision 2008/633/JHA</i>	<i>Article 55e Amendments to Council Decision 2008/633/JHA</i>	
765	1) A new paragraph (1a) is added to Article 5:	1) A new paragraph (1a) is added to Article 5:	1) A new paragraph (1a) is added to Article 5:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
766	"1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the VIS."	1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], <i>and where the conditions for access laid down in this Article are met</i> , they may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the VIS.	"1a. In cases where the designated authorities launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data <i>are</i> is stored in the VIS."	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
767	2) A new point (1a) is added to Article 7:	2) A new point (1a) is added to Article 7:	2) A new point (1a) is added to Article 7:	
768	"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the VIS."	1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], and where the conditions for access laid down in this Article are met, Europol they may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the VIS.	"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access VIS for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data are is stored in the VIS."	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
769	<u>Article 55f</u> <u>Amendments to Regulation (EU) 2018/XX [the ETIAS Regulation]</u>	<i>Article 55f</i> <i>Amendments to Regulation (EU) 2018/XX [the ETIAS Regulation]</i>	<i>Article 55f</i> <i>Amendments to Regulation (EU) 2018/XX [the ETIAS Regulation]</i>	
770	<u>Regulation (EU) 2018/XXX (the ETIAS Regulation) is amended as follows:</u>	Regulation (EU) 2018/XXX (the ETIAS Regulation) is amended as follows:	Regulation (EU) 2018/XXX (the ETIAS Regulation) is amended as follows:	
771	<u>1. In Article 1, the following paragraph is inserted:</u>	1. In Article 1, the following paragraph is inserted:	1. In Article 1, the following paragraph is inserted:	
772	<u>"1a. By storing identity and travel document data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the ETIAS contributes to facilitating and assisting in the correct identification of persons registered in the ETIAS under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."</u>	"1a. By storing identity and travel document data in the common identity repository (CIR) established by [Article 17 of Regulation 2018/XX on interoperability], the ETIAS contributes to facilitating and assisting in the correct identification of persons registered in the ETIAS under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."	"1a. By storing identity and travel document data in the common identity repository (CIR) established by [Article 17(I) of Regulation 2018/XX on interoperability], the ETIAS contributes to facilitating and assisting in the correct identification of persons registered in the ETIAS under the conditions and for the ultimate objectives referred to in [Article 20] of that Regulation."	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
773	<u>2. In Article 3(1), the following points are added:</u>	2. In Article 3(1), the following points are added:	2. In Article 3(1), the following points are added:	
774	<u>"(pa) 'CIR' means the common identity repository as defined in [point 35 of Article 4 of Regulation 2018/XX on interoperability];</u>	"(pa) 'CIR' means the common identity repository as defined in [point 35 of Article 4 of Regulation 2018/XX on interoperability];	"(pa)-(23) 'CIR' means the common identity repository <i>established by</i> as defined in [point 35 of Article 17(1) 4 of Regulation 2018/XX on interoperability];	
775	<u>(pb) 'ETIAS Central System' means the Central System referred to in Article 6(2)(ab) together with the CIR to the extent that the CIR contains the data referred to in Article 6(2a);</u>	(pb) 'ETIAS Central System' means the Central System referred to in Article 6(2)(ab) together with the CIR to the extent that the CIR contains the data referred to in Article 6(2a);	(pb) (24) 'ETIAS Central System' means the Central System referred to in Article 6(2)(ab) together with the CIR to the extent that the CIR contains the data referred to in Article 6(2a);	
776	<u>(pc) 'identity data' means the data referred to in Article 17(2)(a);</u>	(pc) 'identity data' means the data referred to in Article 17(2)(a);	(pe) (25) 'identity data' means the data referred to in <i>points (a), (b) and (c) of</i> Article 17(2)(a);	
777	<u>(pd) 'travel document data' means the data referred to in Article 17(2)(d) and (e) and the three letter code of the country issuing the travel document as referred to in Article 19(3)(c);"</u>	(pd) 'travel document data' means the data referred to in Article 17(2)(d) and (e) and the three letter code of the country issuing the travel document as referred to in Article 19(3)(c);"	(pd) -(26) 'travel document data' means the data referred to in <i>points (d) and (e) of</i> Article 17(2)(d) and (e) and the three letter code of the country issuing the travel document as referred to in <i>point (c) of</i> Article 19(3)(e);".	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
778	<u>3. In Article 4, the following point is added:</u>	3. In Article 4, the following point is added:	3. In Article 4, the following point is added:	
779	<u>"(g) contribute to the correct identification of persons;"</u>	"(g) contribute to the correct identification of persons;"	"(g) contribute to the correct identification of persons;"	
780	<u>4. In Article 6(2), point (a) is replaced by the following:</u>	4. In Article 6(2), point (a) is replaced by the following:	4. In Article 6(2), point (a) is replaced by the following:	
781	<u>"(a) the common identity repository (CIR) as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability];"</u>	"(a) the common identity repository (CIR) as referred to in [Article 17(2)(a) of Regulation 2018/XX on interoperability];"	"(a) the common identity repository (CIR) as referred to in <i>established by</i> [Article 17(1)(2)(a) of Regulation 2018/XX on interoperability];".	
782	<u>5. In Article 6(2) a following point (ab) is inserted:</u>	5. In Article 6(2) a following point (ab) is inserted:	5. In Article 6(2), <i>the</i> a following point (ab) is inserted:	
783	<u>"(ab) a Central System, including the watchlist;"</u>	"(ab) a Central System, including the watchlist;"	"(ab) a Central System, including the <i>ETIAS</i> watchlist, <i>referred to in Article 34;</i> ".	
784	<u>6. In Article 6(2), point (n) is replaced by the following:</u>	6. In Article 6(2), point (n) is replaced by the following:	6. In Article 6(2), point <i>(d)</i> (n) is replaced by the following:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
785	<u>"(n) a secure communication infrastructure between the ETIAS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], the common identity repository established by [Article 17 of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability];"</u>	"(n) a secure communication infrastructure between the ETIAS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], the common identity repository established by [Article 17 of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability];"	"(d#) a secure communication infrastructure between the ETIAS Central System and the central infrastructures of the European search portal established by [Article 6 of Regulation 2018/XX on interoperability], and the CIR common identity repository established by [Article 17(I) of Regulation 2018/XX on interoperability] and the multiple-identity detector established by [Article 25 of Regulation 2018/XX on interoperability];" .	
786	<u>7. In Article 6, the following paragraph is inserted:</u>	7. In Article 6, the following paragraph is inserted:	7. In Article 6, the following paragraph is inserted:	
787	<u>"2a. The CIR shall contain the identity and travel document data referred to in Article 17(2)(a) and (b) to (e) as well as the three letter code of the country issuing the travel document as referred to in Article 19(3)(c), the remaining data shall be stored in the</u>	"2a. The CIR shall contain the identity and travel document data referred to in Article 17(2)(a) and (b) to (e) as well as the three letter code of the country issuing the travel document as referred to in Article 19(3)(c), the remaining data shall be stored in the ETIAS Central System."	"2a. The CIR shall contain the identity and travel document data referred to in points (25) and (26) of Article 3(I) 17(2)(a) and (b) to (e) as well as the three letter code of the country issuing the travel document as referred to in Article 19(3)(c) . The remaining data shall be stored in the ETIAS	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>ETIAS Central System."</u>		Central System."	
788	<u>8. Article 13 is amended as follows:</u>	8. Article 13 is amended as follows:	8. Article 13 is amended as follows:	
789	<u>(a) paragraph 5 is replaced by the following:</u>	(a) paragraph 5 is replaced by the following:	(a) <i>the following</i> paragraph-5 is <i>inserted</i> replaced by the following:	
790	<u>"5. Access to consulting the ETIAS identity and travel document data stored in the CIR shall also be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the EU bodies that are competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and Union bodies in accordance with those purposes and shall be proportionate to</u>	"5. Access to consulting the ETIAS identity and travel document data stored in the CIR shall also be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the EU bodies that are competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and Union bodies in accordance with those purposes and shall be proportionate to the objectives pursued.	"54a. Access to consulting the ETIAS identity and travel document data stored in the CIR shall also be reserved exclusively for the duly authorised staff of the national authorities of each Member State and for the duly authorised staff of the EU <i>agencies</i> bodies that are competent for the purposes laid down in [Article 20 and Article 21 of Regulation 2018/XX on interoperability]. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities and Union <i>agencies</i> bodies in accordance with those purposes and shall be proportionate to the objectives	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>the objectives pursued.</u>		pursued.";	
791			<i>(b) paragraph 5 is replaced by the following:</i>	
792	<u>6. Each Member State shall designate the competent national authorities referred to in paragraphs 1, 2 4 and 5 of this Article and shall communicate a list of these authorities to eu-LISA without delay, in accordance with Article 87(2). That list shall specify for which purpose the duly authorised staff of each authority shall have access to the data in ETIAS Information System in accordance with paragraphs 1, 2 4 and 5 of this Article."</u>	6. Each Member State shall designate the competent national authorities referred to in paragraphs 1, 2 4 and 5 of this Article and shall communicate a list of these authorities to eu-LISA without delay, in accordance with Article 87(2). That list shall specify for which purpose the duly authorised staff of each authority shall have access to the data in ETIAS Information System in accordance with paragraphs 1, 2 4 and 5 of this Article.";	"56. Each Member State shall designate the competent national authorities referred to in paragraphs 1, 2, 4 and 4a 5 of this Article and shall communicate a list of these authorities to eu-LISA without delay, in accordance with Article 87(2). That list shall specify for which purpose the duly authorised staff of each authority shall have access to the data in ETIAS Information System in accordance with paragraphs 1, 2, 4 and 4a 5 of this Article ;".	
793	<u>9. In Article 17(2), point (a) is replaced by the following:</u>	9. In Article 17(2), point (a) is replaced by the following:	9. In Article 17(2) is <i>amended as follows</i> , point (a) is replaced by the following:	
794			<i>(a) point (a) is replaced by the following:</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
795	<u>"(a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality;"</u>	"(a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality;	"(a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality;"	
796			<i>(b) the following point is inserted:</i>	
797	<u>(ab) country of birth, first name(s) of the parents of the applicant;"</u>	(ab) country of birth, first name(s) of the parents of the applicant;"	"(ab) country of birth, first name(s) of the parents of the applicant;"	
798	<u>10. In Article 19(4) the words "Article 17(2)(a)" are replaced by the words " Article 17(2)(a) and (ab)".</u>	10. In Article 19(4) the words "Article 17(2)(a)" are replaced by the words " Article 17(2)(a) and (ab)".	10. In Article 19(4) the words " <i>point (a) of</i> Article 17(2)(a)" are replaced by the words " <i>points (a) and (ab) of</i> Article 17(2)(a) and (ab)".	
799	<u>11. Article 20 is amended as follows:</u>	11. Article 20 is amended as follows:	11. Article 20 is amended as follows:	
800	<u>(a) in paragraph 2, the first subparagraph is replaced by the following:</u>	(a) in paragraph 2, the first subparagraph is replaced by the following:	(a) in paragraph 2, the first subparagraph is replaced by the following:	
801	<u>"2. The ETIAS Central System shall launch a query by using the European Search Portal defined in [Article 6(1) of the</u>	"2. The ETIAS Central System shall launch a query by using the European Search Portal defined in [Article 6(1) of the	"2. The ETIAS Central System shall launch a query by using the European Search Portal defined <i>in-established by</i> [Article 6(1) of	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>Interoperability Regulation] to compare the relevant data referred to in Article 17(2)(a), (ab), (b), (c), (d),(f),(g), (j), (k), (m) and (8) to the data present in a record, file or alert registered in an application file stored in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol databases SLTD and TDAWN."</u>	Interoperability Regulation] to compare the relevant data referred to in Article 17(2)(a), (ab), (b), (c), (d),(f),(g), (j), (k), (m) and (8) to the data present in a record, file or alert registered in an application file stored in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol databases SLTD and TDAWN."	the Interoperability Regulation] to compare the relevant data referred to in <i>points (a), (ab), (b), (c), (d), (f), (g), (j), (k) and (m) of</i> Article 17(2)(a), (ab), (b), (c), (d),(f),(g), (j), (k), (m) and <i>in Article 17(8)</i> to the data present in a record, file or alert registered in an application file stored in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol databases SLTD and TDAWN."	
802	<u>(b) In paragraph 4 the words "Article 17(2)(a), (b), (c), (d), (f), (g), (j), (k), (m) and (8)" are replaced by the words "Article 17(2)(a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) and (8)".</u>	(b) In paragraph 4 the words "Article 17(2)(a), (b), (c), (d), (f), (g), (j), (k), (m) and (8)" are replaced by the words "Article 17(2)(a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) and (8)".	(b) In paragraph 4, the words " <i>points (a), (b), (c), (d), (f), (g), (j), (k) and (m) of</i> Article 17(2)(a), (b), (c), (d), (f), (g), (j), (k), (m) and Article 17(8)" are replaced by the words " <i>points (a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) of</i> Article 17(2)(a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) and Article 17(8)".	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
803	<u>(c) In paragraph 5 the words "Article 17(2)(a), (b), (c), (d), (f), (g), (j), (k), (m) and (8)" are replaced by the words "Article 17(2)(a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) and (8)".</u>	(c) In paragraph 5 the words "Article 17(2)(a), (b), (c), (d), (f), (g), (j), (k), (m) and (8)" are replaced by the words "Article 17(2)(a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) and (8)".	(c) In paragraph 5, the words " <i>points (a), (c), (f), (h) and (i) of Article 17(2)(a), (b), (c), (d), (f), (g), (j), (k), (m) and (8)</i> " are replaced by the words " <i>points (a), (ab), (c), (f), (h) and (i) of Article 17(2)(a), (ab), (b), (c), (d), (f), (g), (j), (k), (m) and (8)</i> ".	
804	<u>12. Article 23(1), is replaced by the following:</u>	12. Article 23(1), is replaced by the following:	12. <i>In</i> Article 23(1), <i>paragraph 1</i> is replaced by the following:	
805	<u>"1. The ETIAS Central System shall launch a query by using the European Search Portal defined in [Article 6(1) of the Interoperability Regulation] to compare the relevant data referred to in Article 17(2)(a), (ab), (b) and (d) to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts:</u>	"1. The ETIAS Central System shall launch a query by using the European Search Portal defined in [Article 6(1) of the Interoperability Regulation] to compare the relevant data referred to in Article 17(2)(a), (ab), (b) and (d) to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts:	"1. The ETIAS Central System shall launch a query by using the European Search Portal defined <i>in-established by</i> [Article 6(1) of the Interoperability Regulation] to compare the relevant data referred to in <i>points (a), (ab), (b) and (d) of Article 17(2)(a), (ab), (b) and (d) and the three letter code of the country issuing the travel document as referred to in point (c) of Article 19(3)</i> to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>access the application files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the application files stored in the ETIAS Central System."</u>	files stored in the ETIAS Central System in accordance with this [Article 45] for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the application files stored in the ETIAS Central System."	files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data is stored in the application files stored in the ETIAS Central System."	
812	<u>15. In Article 53, the following paragraph is inserted:</u>	15. In Article 53, the following paragraph is inserted:	15. In Article 53, the following paragraph is inserted:	
813	<u>"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access the application files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that</u>	"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access the application files stored in the ETIAS Central System in accordance with this [Article 46] for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data	"1a. In cases where Europol launched a query to the CIR in accordance with [Article 22 of Regulation 2018/XX on interoperability], they may access the application files stored in the ETIAS Central System in accordance with this Article for consultation where the reply received as referred to in paragraph 3 of [Article 22 of Regulation 2018/XX on interoperability] reveals that data	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>data is stored in the application files stored in the ETIAS Central System."</u>	is stored in the application files stored in the ETIAS Central System."	is stored in the application files stored in the ETIAS Central System."	
814			<i>15a. In Article 54, a new paragraph is added:</i>	
815			<i>"3a. Where a red link is stored in the multiple identity detector (MID) established by [Article 25 of Regulation 2018/XX on interoperability] in accordance with [Article 32 of Regulation 2018/XX on interoperability], the linked ETIAS data referred to in points (a), (b), (c), (d) and (e) of Article 17(2) shall be stored in the CIR in accordance with [Article 23(3) of Regulation 2018/XX on interoperability]."</i>	
816	<u>16. In Article 65(3) fifth subparagraph, the words "Article 17(2)(a), (b), (d), (e) and (f)" are replaced by the words "Article 17(2)(a), (ab), (b), (d), (e) and (f)".</u>	16. In Article 65(3) fifth subparagraph, the words "Article 17(2)(a), (b), (d), (e) and (f)" are replaced by the words "Article 17(2)(a), (ab), (b), (d), (e) and (f)".	16. In <i>the fifth subparagraph of Article 65(3) fifth subparagraph</i> , the words "points (a), (b), (d), (e) and (f) of Article 17(2)(a), (b), (d), (e) and (f)" are replaced by the words "points (a), (ab), (b), (d), (e) and (f) of Article 17(2)(a), (ab), (b), (d), (e) and (f)".	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			(€)".	
817	<u>17. In Article 69(1), the following point is inserted:</u>	17. In Article 69(1), the following point is inserted:	17. In Article 69(1), the following point is inserted:	
818	<u>"(ca) where relevant, a reference to the use of the European search portal to query the ETIAS Central System as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability],"</u>	"(ca) where relevant, a reference to the use of the European search portal to query the ETIAS Central System as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability],"	"(ca) where relevant, a reference to the use of the European search portal to query the ETIAS Central System as referred to in [Article 7(2) of the Regulation 2018/XX on interoperability],".	
819	<u>18. In Article 73(2), the words "the central repository of data" are replaced by the words "the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability] to the extent that it contains data obtained from the ETIAS Central System in accordance with Article 84".</u>	18. In Article 73(2), the words "the central repository of data" are replaced by the words "the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability] to the extent that it contains data obtained from the ETIAS Central System in accordance with Article 84".	18. In Article 73(2), the words "the central repository of data" are replaced by the words "the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability] to the extent that it contains data obtained from the ETIAS Central System in accordance with Article 84".	
820	<u>19. In Article 74(1), the words "and the central repository of data, as referred</u>	19. In Article 74(1), the words "and the central repository of data, as referred to in Article	19. In Article 74(1), the words "and the central repository of data, as referred to in Article	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>to in Article 6" are deleted.</u>	6" are deleted.	6" are deleted.	
821	<u>20. In Article 84(2), the first subparagraph is replaced by the following:</u>	20. In Article 84(2), the first subparagraph is replaced by the following:	20. In Article 84(2), the first subparagraph is replaced by the following:	
822	<u>"2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]. In accordance with [Article 39(1) of the Regulation 2018/XX on interoperability], cross-system statistical data and analytical reporting would allow the authorities listed in paragraph 1 to obtain customisable reports and statistics, to support the implementation of the ETIAS screening rules referred to in Article 33, to improve the assessment of the security, illegal immigration and high epidemic risks, to</u>	"2. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]. In accordance with [Article 39(1) of the Regulation 2018/XX on interoperability], cross-system statistical data and analytical reporting would allow the authorities listed in paragraph 1 to obtain customisable reports and statistics, to support the implementation of the ETIAS screening rules referred to in Article 33, to improve the assessment of the security, illegal immigration and high epidemic risks, to enhance the efficiency of border checks and to help the	"2. For the purpose of paragraph 1 of this Article , eu-LISA shall store the data referred to in paragraph 1 in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]. In accordance with [Article 39(1) of the Regulation 2018/XX on interoperability], cross-system statistical data and analytical reporting <i>shall would</i> allow the authorities listed in paragraph 1 to obtain customisable reports and statistics, to support the implementation of the ETIAS screening rules referred to in Article 33, to improve the assessment of the security, illegal immigration and high epidemic risks, to enhance the efficiency of border checks and to help the	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>enhance the efficiency of border checks and to help the ETIAS Central Unit and the ETIAS National Units process the travel authorisation applications."</u>	ETIAS Central Unit and the ETIAS National Units process the travel authorisation applications."	ETIAS Central Unit and the ETIAS National Units process the travel authorisation applications."	
823	<u>21. In Article 84(4), a new subparagraph is added:</u>	21. In Article 84(4), a new subparagraph is added:	21. In Article 84(4), a new second subparagraph is added:	
824	<u>"The daily statistics shall be stored in the central repository for reporting and statistics."</u>	"The daily statistics shall be stored in the central repository for reporting and statistics."	"The daily statistics shall be stored in the central repository for reporting and statistics."	
825	<u>Article 55g Amendments to Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks]</u>	<i>Article 55g Amendments to Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks]</i>	<i>Article 55g Amendments to Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks]</i>	
826	<u>Regulation (EU) 2018/XX is amended as follows:</u>	Regulation (EU) 2018/XX is amended as follows:	Regulation (EU) 2018/XX is amended as follows:	
827	<u>1. In Article 3(1), the following points are added:</u>	1. In Article 3(1), the following points are added:	1. In Article 3(1), the following points are added:	
828	<u>“(t) ‘ESP’ means the European search portal as defined in [Article 6 of Regulation 2018/XX on interoperability].</u>	“(t) ‘ESP’ means the European search portal as defined in [Article 6 of Regulation 2018/XX on interoperability].	“(t 2 3) ‘ESP’ means the European search portal as defined in established by [Article 6(1) of Regulation 2018/XX on interoperability].	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
829	<u>(u) 'shared BMS' means the shared biometric matching service as defined in [Article 12 of Regulation 2018/XX on interoperability].</u>	(u) 'shared BMS' means the shared biometric matching service as defined in [Article 12 of Regulation 2018/XX on interoperability].	(u24) 'shared BMS' means the shared biometric matching service as defined in <i>established by</i> [Article 12(1) of Regulation 2018/XX on interoperability].	
830	<u>(v) 'CIR' means the common identity repository as referred to in [Article 17 of Regulation 2018/XX on interoperability];</u>	(v) 'CIR' means the common identity repository as referred to in [Article 17 of Regulation 2018/XX on interoperability];	(v25) 'CIR' means the common identity repository as referred to in <i>established by</i> [Article 17(1) of Regulation 2018/XX on interoperability];	
831	<u>(w) 'MID' means the multiple-identity detector as defined in [Article 25 of Regulation 2018/XX on interoperability].</u>	(w) 'MID' means the multiple-identity detector as defined in [Article 25 of Regulation 2018/XX on interoperability].	(w26) 'MID' means the multiple-identity detector as defined in <i>established by</i> [Article 25(1) of Regulation 2018/XX on interoperability].	
832	<u>2. Article 4 is amended as follows:</u>	2. Article 4 is amended as follows:	2. Article 4 is amended as follows:	
833	<u>(a) in paragraph 3, the following point (d) is added:</u>	(a) in paragraph 3, the following point (d) is added:	(a) in paragraph 1 3, the following point (d) is added:	
834	<u>"d) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP, the shared BMS and the MID "</u>	"d) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP, the shared BMS and the MID "	" (d) e) a secure communication infrastructure between CS-SIS and the central infrastructures of the ESP <i>established by [Article 6 of Regulation 2018/XX on interoperability]</i> , the shared BMS	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>established by [Article 12 of Regulation 2018/XX on interoperability] and the MID established by [Article 25 of Regulation 2018/XX on interoperability] "</i> .	
835	<u>(b) the following paragraphs are added:</u>	(b) the following paragraphs are added:	(b) the following paragraphs are added:	
836	<u>“5. Without prejudice to paragraphs (1) to (4) of this Article, SIS data may also be searched via the ESP.</u>	“5. Without prejudice to paragraphs (1) to (4) of this Article, SIS data may also be searched via the ESP.	“ 85 . Without prejudice to paragraphs (1) to (5) (4) of this Article, SIS data may also be searched via the ESP.	
837	<u>6. Without prejudice to paragraphs (1) to (4) of this Article, SIS data may also be transmitted via the secure communication infrastructure defined in paragraph (3)(d) of this Article. These transmissions shall be limited to the extent that the data are required for the functionalities referred to in [Regulation 2018/XX on interoperability].”</u>	6. Without prejudice to paragraphs (1) to (4) of this Article, SIS data may also be transmitted via the secure communication infrastructure defined in paragraph (3)(d) of this Article. These transmissions shall be limited to the extent that the data are required for the functionalities referred to in [Regulation 2018/XX on interoperability].”	96 . Without prejudice to paragraphs (1) to (5) (4) of this Article, SIS data may also be transmitted via the secure communication infrastructure defined in <i>point (e)</i> of paragraph (1) (3)(d) of this Article. These transmissions shall be limited to the extent that the data are required for the functionalities referred to in [Regulation 2018/XX on interoperability].”	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
838	<u>3. In Article 7 the following paragraph 2a is added:</u>	3. In Article 7 the following paragraph 2a is added:	3. In Article 7, the following paragraph 2a is <i>inserted</i> added:	
839	<u>"2a. The SIRENE Bureaux shall also ensure the verification of different identities in accordance with [Article 29 Regulation 2018/XX on interoperability]. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to consulting the data stored in the CIR for the purposes laid down in [Article 21 of Regulation 2018/XX on interoperability]."</u>	"2a. The SIRENE Bureaux shall also ensure the verification of different identities in accordance with [Article 29 Regulation 2018/XX on interoperability]. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to consulting the data stored in the CIR for the purposes laid down in [Article 21 of Regulation 2018/XX on interoperability]."	"2a. The SIRENE Bureaux shall also ensure the verification of different identities in accordance with [Article 29 Regulation 2018/XX on interoperability]. To the extent necessary to carry out this task, the SIRENE Bureaux shall have access to consulting the data stored in the CIR <i>and the MID</i> for the purposes laid down in [Articles 21 <i>and 26</i> of Regulation 2018/XX on interoperability]."	
840	<u>4. in Article 8 paragraph 4 is deleted.</u>	4. in Article 8 paragraph 4 is deleted.	4. in Article 8 paragraph 4 is deleted.	
841	<u>5. in Article 12 paragraph 1 is replaced by the following:</u>	5. in Article 12 paragraph 1 is replaced by the following:	5. In Article 12, paragraph 1 is replaced by the following:	
842	<u>"1. Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS for the purposes of</u>	"1. Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS for the purposes of checking	"1. Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS for the purposes of checking	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS, data integrity and security. This does not apply to the automatic processes referred to in Article 4(4) (a), (b) and (c). Member States shall ensure that every access to personal data via the ESP are also logged for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring, data integrity and security.</u>	whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS, data integrity and security. This does not apply to the automatic processes referred to in Article 4(4) (a), (b) and (c). Member States shall ensure that every access to personal data via the ESP are also logged for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring, data integrity and security.”	whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS, data integrity and security. This does not apply to the automatic processes referred to in <i>points (a), (b) and (c) of</i> Article 4(4) (a), (b) and (c) . Member States shall ensure that every access to personal data via the ESP are also logged for the purposes of checking whether or not the search is lawful, monitoring the lawfulness of data processing, self-monitoring, data integrity and security.”	
843	<u>6. In Article 29(1), the following point (g) is added:</u>	6. In Article 29(1), the following point (g) is added:	56. In Article 29-34 (1), the following point (g) is added:	
844	<u>“(g) verifying different identities and combating identity fraud in accordance with [Chapter V of Regulation 2018/XX on interoperability].”</u>	“(g) verifying different identities and combating identity fraud in accordance with [Chapter V of Regulation 2018/XX on interoperability].”	“(g) verifying different identities and combating identity fraud in accordance with [Chapter V of Regulation 2018/XX on interoperability].”	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
845	<u>7. in Article 54 paragraph 6, is replaced by the following:</u>	7. in Article 54 paragraph 6, is replaced by the following:	67. In Article 54 60 , paragraph 6; is replaced by the following:	
846	<u>"For the purpose of paragraphs 3, 4 and 5 of this Article and of Article 15(5), the Agency shall store data referred to in paragraph 3 of this Article and in Article 15(5) which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability]."</u>	"For the purpose of paragraphs 3, 4 and 5 of this Article and of Article 15(5), the Agency shall shall store data referred to in paragraph 3 of this Article and in Article 15(5) which shall not allow for the identification of individuals in the central repository for reporting and statistics <i>establish, implement and host a central repository in its technical sites containing the data referred to in paragraph 3 of this Article and in Article 15(5) which shall not allow for the identification of individuals and shall allow the Commission and the agencies referred to in paragraph 5 to obtain bespoke reports and statistics</i> referred to in [Article 39 of the Regulation 2018/XX on interoperability].	"6. For the purpose of paragraphs 3, 4 and 5 of this Article and of Article 15(5), the Agency shall store data referred to in paragraph 3 of this Article and in Article 15(5) which shall not allow for the identification of individuals in the central repository for reporting and statistics referred to in [Article 39 of the Regulation 2018/XX on interoperability].	
847	<u>The Agency shall allow the Commission and the agencies</u>	The Agency shall allow the Commission and the agencies	The Agency shall allow the Commission and the agencies	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>referred to in paragraph 5 to obtain bespoke reports and statistics. Upon request, the Agency shall give access to Member States, the Commission, Europol, and the European Border and Coast Guard Agency to the central repository in accordance with [Article 39 of the Regulation 2018/XX on interoperability]."</u>	referred to in paragraph 5 to obtain bespoke reports and statistics. Upon request, the Agency shall give access to Member States, the Commission, Europol, and the European Border and Coast Guard Agency to the central repository in accordance with [Article 39 of the Regulation 2018/XX on interoperability] . <i>to the extent required for the performance of their tasks, to the central repository by means of secured access through the Communication Infrastructure with control of access and specific user profiles solely for the purpose of reporting and statistics."</i>	<i>bodies</i> referred to in paragraph 5 to obtain bespoke reports and statistics. Upon request, the Agency shall give access to Member States, the Commission, Europol, and the European Border and Coast Guard Agency to the central repository in accordance with [Article 39 of the Regulation 2018/XX on interoperability]."	
848	<u>Article 55h</u> <u>Amendments to Regulation (EU) 2018/XX [Regulation on eu-LISA]</u>	<i>Article 55h</i> <i>Amendments to Regulation (EU) 2018/XX [Regulation on eu-LISA]</i>	<i>Article 55h</i> <i>Amendments to Regulation (EU) 2018/XX [Regulation on eu-LISA]</i>	
849	<u>Regulation (EU) 2018/XX (eu-LISA) is amended as follows:</u>	Regulation (EU) 2018/XX (eu-LISA) is amended as follows:	Regulation (EU) 2018/XX (eu-LISA) is amended as follows:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
850	<u>1. Article 8 is replaced by the following:</u>	1. Article 8 is replaced by the following:	1. Article 12 § is replaced by the following:	
851	<i><u>"Article 8 Data quality</u></i>	<i>"Article 8 Data quality</i>	<i>"Article 12 § Data quality</i>	
852	<u>1. eu-LISA shall establish for all systems under the Agency's operational responsibility automated data quality control mechanisms and procedures and common data quality indicators and the minimum quality standards to store data, in accordance with the relevant provisions of the systems' instruments and of [Article 37 of Regulation 2018/XX on interoperability].</u>	1. eu-LISA shall establish for all systems under the Agency's operational responsibility automated data quality control mechanisms and procedures and common data quality indicators and the minimum quality standards to store data, in accordance with the relevant provisions of the systems' instruments and of [Article 37 of Regulation 2018/XX on interoperability].	1. <i>Without prejudice to Member States' responsibilities with regard to the data entered into the systems under eu-LISA's operational responsibility, eu-LISA, closely involving its Advisory Groups, shall establish for all systems under the Agency's operational responsibility automated data quality control mechanisms and procedures and common data quality indicators and the minimum quality standards to store data, in accordance with the relevant provisions of the systems' instruments and of [Article 37 of Regulation 2018/XX on interoperability].</i>	
853	<u>2. eu-LISA shall establish a central repository for reporting and statistics in accordance</u>	2. eu-LISA shall establish a central repository for reporting and statistics in accordance with	2. eu-LISA shall establish a central repository <i>containing only anonymised data</i> for	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>with [Article 39 of Regulation 2018/XX on interoperability]."</u>	[Article 39 of Regulation 2018/XX on interoperability]."	reporting and statistics <i>subject to specific provisions in the legislative instruments governing the development, establishment, operation and use of large-scale IT systems managed by eu-LISA</i> in accordance with [Article 39 of Regulation 2018/XX on interoperability]."	
854	<u>2. Article 9 is replaced by the following:</u>	2. Article 9 is replaced by the following:	2. Article 9 13 9 is replaced by the following:	
855	<u>"Article 9 Interoperability</u>	"Article 9 Interoperability	"Article 13 9 Interoperability	
856	<u>Where the interoperability of large-scale IT systems has been stipulated in a relevant legislative instrument the Agency shall develop the necessary actions conferred on it by those legislative instruments to enable that interoperability."</u>	Where the interoperability of large-scale IT systems has been stipulated in a relevant legislative instrument the Agency shall develop the necessary actions conferred on it by those legislative instruments to enable that interoperability."	Where the interoperability of large-scale IT systems has been stipulated in a relevant legislative instrument the Agency shall develop the necessary actions conferred on it by those legislative instruments to enable that interoperability."	
857	<u>3. Article 15 is amended as follows:</u>	3. Article 15 is amended as follows:	3. Article 15 19 45(1) is amended as follows:	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
858	<u>(a) paragraph (1) is amended as follows:</u>	(a) paragraph (1) is amended as follows:	(a) — paragraph (1) is amended as follows:	
859	<u>(i) the following point (eea) is inserted:</u>	(i) the following point (eea) is inserted:	(a) (i) the following point (eea) is inserted:	
860	<u>"(eea) Adopt the reports on the state of play of the development of the interoperability components pursuant to [Article 68(2) of Regulation 2018/XX on interoperability]."</u>	"(eea) Adopt the reports on the state of play of the development of the interoperability components pursuant to [Article 68(2) of Regulation 2018/XX on interoperability]."	"(eea) a Adopt the reports on the state of play of the development of the interoperability components pursuant to [Article 68(2) of Regulation 2018/XX on interoperability].";	
861	<u>(ii) point (ff) is replaced by the following:</u>	(ii) point (ff) is replaced by the following:	(b) (ii) point (ff) is replaced by the following:	
862	<u>"(ff) 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/JHA respectively [or Article 54(7) of Regulation 2018/XX of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks,</u>	"(ff) 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/JHA respectively [or Article 54(7) of Regulation 2018/XX of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending	"(ff) 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/JHA respectively [or Article 54(7) of Regulation 2018/XX of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p><u>amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006 and Article 71(7) of Regulation 2018/XX of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU], of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, of ETIAS pursuant to Article 81(4) of Regulation (EU) 2018/XX on the ECRIS-TCN system and the ECRIS reference implementation</u></p>	<p>Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006 and Article 71(7) of Regulation 2018/XX of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU], of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, of ETIAS pursuant to Article 81(4) of Regulation (EU) 2018/XX on the ECRIS-TCN system and the ECRIS reference implementation pursuant to Article 34(4) of Regulation (EU) 2018/XX] and</p>	<p>Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006 and Article 71(7) of Regulation 2018/XX of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU], of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, of ETIAS pursuant to Article 92 84(4), of Regulation (EU) 2018/XX on the ECRIS-TCN system and the ECRIS reference implementation pursuant to Article 34(4) of Regulation (EU)</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>pursuant to Article 34(4) of Regulation (EU) 2018/XX] and of the interoperability components pursuant to [Article 68(4) of Regulation 2018/XX on interoperability];"</u>	of the interoperability components pursuant to [Article 68(4) of Regulation 2018/XX on interoperability];"	2018/XX] and of the interoperability components pursuant to [Article 68(4) of Regulation 2018/XX on interoperability];"	
863	<u>(iii) point (hh) is replaced by the following:</u>	(iii) point (hh) is replaced by the following:	(ciii) point (hh) is replaced by the following:	
864	<u>"(hh) adopt formal comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, and [Article 57 of Regulation (EU) 2018/XX (establishing the ETIAS)] and to [Article 27(2) of Regulation (EU) 2018/XX (establishing the ECRIS-TCN system)] and to [Article 50 of Regulation 2018/XX on interoperability] and ensure appropriate follow-</u>	"(hh) adopt formal comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, and [Article 57 of Regulation (EU) 2018/XX (establishing the ETIAS)] and to [Article 27(2) of Regulation (EU) 2018/XX (establishing the ECRIS-TCN system)] and to [Article 50 of Regulation 2018/XX on interoperability] and ensure appropriate follow-up of those audits;"	"(hh) adopt formal comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45(2) of Regulation (EC) No 1987/2006, Article 42(2) of Regulation (EC) No 767/2008 and Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, and [Article 57 67 of Regulation (EU) 2018/XX (establishing the ETIAS)] and to [Article 27(2) of Regulation (EU) 2018/XX (establishing the ECRIS-TCN system)] and to [Article 50 of Regulation 2018/XX on interoperability] and ensure appropriate follow-up of those audits;"	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>up of those audits;"</u>			
865			<i>(d) point (mm) is replaced by the following:</i>	
866			<i>"(mm) ensure annual publication of the list of competent authorities authorised to search directly the data contained in SIS II pursuant to Article 31(8) of Regulation (EC) No 1987/2006 and Article 46(8) of Decision 2007/533/JHA, together with the list of Offices of the national systems of SIS II (N.SIS II) and SIRENE Bureaux pursuant to Article 7(3) of Regulation (EC) No 1987/2006 and Article 7(3) of Decision 2007/533/JHA respectively as well as the list of competent authorities pursuant to Article 65(2) of Regulation (EU) 2017/2226 and, the list of competent authorities pursuant to Article 87(2) of Regulation (EU) 2018/...⁺, [the list of</i>	

⁺ OJ: Please insert serial number of the Regulation in 2016/0357A(COD).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>competent authorities pursuant to Article 32 of Regulation (EU) 2018/... (ECRIS-TCN)] and the list of authorities pursuant to Article 61(1) of [Regulation (EU) 2018/... on interoperability]."</i>	
867	<u>4. In Article 19 paragraph 4 is replaced by the following:</u>	4. In Article 19 paragraph 4 is replaced by the following:	4. In Article 22 19, paragraph 4 is replaced by the following:	
868	<u>"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. [The European Border and Coast Guard Agency may attend the meetings of the Management Board as observers when a question concerning SIS in relation to the application of Regulation (EU) 2016/1624 is on the agenda]. Europol may also attend the meetings of the</u>	"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. [The European Border and Coast Guard Agency may attend the meetings of the Management Board as observers when a question concerning SIS in relation to the application of Regulation (EU) 2016/1624 is on the agenda]. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS,	"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. [The European Border and Coast Guard Agency may attend the meetings of the Management Board as observers when a question concerning SIS in relation to the application of Regulation (EU) 2016/1624 is on the agenda]. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS,	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<p><u>Management Board as observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, is on the agenda. Europol may also attend the meetings of the Management Board as an observer when a question concerning EES in relation to the application of Regulation (EU) 2017/2226 is on the agenda or when a question concerning ETIAS in relation to Regulation 2018/XX (establishing ETIAS) is on the agenda. The European Border and Coast Guard Agency may also attend the meetings of the Management Board as observer when a question concerning ETIAS in relation with the application of Regulation 2018/XX (establishing ETIAS) is on the agenda.] [EASO may</u></p>	<p>in relation to the application of Decision 2008/633/JHA, or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, is on the agenda. Europol may also attend the meetings of the Management Board as an observer when a question concerning EES in relation to the application of Regulation (EU) 2017/2226 is on the agenda or when a question concerning ETIAS in relation to Regulation 2018/XX (establishing ETIAS) is on the agenda. The European Border and Coast Guard Agency may also attend the meetings of the Management Board as observer when a question concerning ETIAS in relation with the application of Regulation 2018/XX (establishing ETIAS) is on the agenda.] [EASO may also attend the meetings of the Management Board as an observer when a question concerning the</p>	<p>in relation to the application of Decision 2008/633/JHA, or a question concerning Eurodac, in relation to the application of Regulation (EU) No 603/2013, is on the agenda. Europol may also attend the meetings of the Management Board as an observer when a question concerning EES in relation to the application of Regulation (EU) 2017/2226 is on the agenda or when a question concerning ETIAS in relation to Regulation 2018/XX (establishing ETIAS) is on the agenda. [The European Border and Coast Guard Agency may also attend the meetings of the Management Board as observer when a question concerning ETIAS in relation with the application of Regulation 2018/XX (establishing ETIAS) is on the agenda.] [EASO may also attend the meetings of the Management Board as an observer when a question concerning the</p>	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
	<p><u>also attend the meetings of the Management Board as an observer when a question concerning the automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) COM(2016) 270 final-2016/0133(COD), is on the agenda.] [Eurojust, Europol [the European Public Prosecutor's Office] may also attend the meetings of the Management Board as observers when a question concerning Regulation 2018/XX (establishing a centralised system for the identification of</u></p>	<p>automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) COM(2016) 270 final-2016/0133(COD), is on the agenda.] [Eurojust, Europol [the European Public Prosecutor's Office] may also attend the meetings of the Management Board as observers when a question concerning Regulation 2018/XX (establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (TCN) to</p>	<p>automated system for registration, monitoring and the allocation mechanism for applications for international protection referred to in Article 44 of Regulation (EU) establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) COM(2016) 270 final-2016/0133(COD), is on the agenda.][Eurojust, Europol [the European Public Prosecutor's Office] may also attend the meetings of the Management Board as observers when a question concerning Regulation 2018/XX (establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (TCN) to</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>Member States holding conviction information on third-country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS), and amending Regulation (EU) No 1077/2011 (ECRIS-TCN system) is on the agenda.] Europol, Eurojust and the European Border and Coast Guard Agency may also attend the meetings of the Management Board as observers when a question concerning [Regulation 2018/XX on interoperability] is on the agenda. The Management Board may invite any other person whose opinion may be of interest, to attend its meetings as an observer."</u>	supplement and support the European Criminal Records Information System (ECRIS), and amending Regulation (EU) No 1077/2011 (ECRIS-TCN system) is on the agenda.] Europol, Eurojust and the European Border and Coast Guard Agency may also attend the meetings of the Management Board as observers when a question concerning [Regulation 2018/XX on interoperability] is on the agenda. The Management Board may invite any other person whose opinion may be of interest, to attend its meetings as an observer."	supplement and support the European Criminal Records Information System (ECRIS), and amending Regulation (EU) No 1077/2011 (ECRIS-TCN system) is on the agenda.] Europol, Eurojust and the European Border and Coast Guard Agency may also attend the meetings of the Management Board as observers when a question concerning [Regulation 2018/XX on interoperability] is on the agenda. The Management Board may invite any other person whose opinion may be of interest, to attend its meetings as an observer."	
869	<u>5. In Article 21(3), point (o) is replaced by the following:</u>	5. In Article 21(3), point (o) is replaced by the following:	5. In Article 21 24 (3), point (o p) is replaced by the following:	
870	<u>"(o) without prejudice to Article 17 of the Staff</u>	"(o) without prejudice to Article 17 of the Staff Regulations,	"(o p) without prejudice to Article 17 of the Staff Regulations,	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	<u>Regulations, establishing confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008 Article 4(4) of Regulation (EU) No 603/2013; Article 37(4) of Regulation 2017/2226, [Article 64(2) of Regulation 2018/XX (establishing the ETIAS)], [Article 11(16) of Regulation 2018/XX (establishing the ECRIS-TCN system)] and [Article 53(2) of Regulation 2018/XX on interoperability];"</u>	establishing confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008 Article 4(4) of Regulation (EU) No 603/2013; Article 37(4) of Regulation 2017/2226, [Article 64(2) of Regulation 2018/XX (establishing the ETIAS)], [Article 11(16) of Regulation 2018/XX (establishing the ECRIS-TCN system)] and [Article 53(2) of Regulation 2018/XX on interoperability];"	establishing confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA, Article 26(9) of Regulation (EC) No 767/2008 Article 4(4) of Regulation (EU) No 603/2013; Article 37(4) of Regulation 2017/2226, [Article 74 64(2) of Regulation 2018/XX (establishing the ETIAS)], [Article 11(16) of Regulation 2018/XX (establishing the ECRIS-TCN system)] and [Article 53(2) of Regulation 2018/XX on interoperability];".	
871	<u>6. Article 23 is amended as follows:</u>	6. <i>In</i> Article 23, is amended as follows: paragraph 3 is replaced by the following:	6. Article 27 23 is amended as follows:	
872	<u>(a) In paragraph 1 the following point is inserted:</u>	(a) In paragraph 1 the following point is inserted:	(a) In paragraph 1, the following point is inserted:	
873	<u>"(ea) Interoperability Advisory Group;"</u>	"(ea) Interoperability Advisory Group;"	"(ea) Interoperability Advisory Group;"	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
874	<u>(b) paragraph 3 is replaced by the following:</u>	(b) paragraph 3 is replaced by the following:	(b) paragraph 3 is replaced by the following:	
875	<u>"3. Europol and Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and Eurodac and EES[-ETIAS] Advisory Groups. The European Border and Coast Guard Agency may also appoint a representative to the EES[-ETIAS] Advisory Group.] [Eurojust, Europol, and the European Public Prosecutors Office] may also appoint a representative to the ECRIS-TCN system Advisory Group.] Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the Interoperability Advisory Group."</u>	"3. Europol and Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and Eurodac and EES[-ETIAS] Advisory Groups. The European Border and Coast Guard Agency may also appoint a representative to the EES[-ETIAS] Advisory Group.] [Eurojust, Europol, and the European Public Prosecutors Office] may also appoint a representative to the ECRIS-TCN system Advisory Group.] Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the Interoperability Advisory Group."	"3. Europol and Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and Eurodac and EES[-ETIAS] Advisory Groups. The European Border and Coast Guard Agency may also appoint a representative to the EES[-ETIAS] Advisory Group.] [Eurojust, Europol, and the European Public Prosecutors Office] may also appoint a representative to the ECRIS-TCN system Advisory Group.] Europol, Eurojust and the European Border and Coast Guard Agency may each appoint a representative to the Interoperability Advisory Group."	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
876	CHAPTER X Final provisions	CHAPTER X Final provisions	CHAPTER X Final provisions	
877			<i>Article 55i Business Continuity</i>	
878			<i>Interoperability of central EU information systems supported by this Regulation shall be accompanied by business continuity solutions, determined and implemented in accordance with [Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011], that ensure uninterrupted availability of all interoperability components and the data stored therein. In order to ensure operational needs, the</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>Commission, in close cooperation with the Member States and eu-LISA, shall adopt the implementing acts necessary for the development and technical implementation of such solutions.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
879		<i>Article -56 Access by third country jurisdictions</i>		
880		<i>With reference to Article 48 of Regulation (EU) 2016/679, Directive (EU) 2016/680, and Articles XIV and XIV bis of the General Agreement on Trade in Services, companies present in a third country jurisdiction where they may be subject to (court) orders or subpoenas by third country authorities requiring them to retrieve data from the interoperability components or different information systems made interoperable, shall be excluded from preparing, designing, developing, hosting or managing any part of an interoperability component, or processing personal data of these systems.</i>		
881	<i>Article 56 Reporting and statistics</i>	<i>Article 56 Reporting and statistics</i>	<i>Article 56 Reporting and statistics</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
882	1. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the European search portal (ESP), solely for the purposes of reporting and statistics without enabling individual identification:	1. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the European search portal (ESP), solely for the purposes of reporting and statistics without enabling individual . <i>The use of these data shall not allow for the identification of a person:</i>	1. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the European search portal (ESP), solely for the purposes of reporting and statistics without enabling individual identification:	
883	(a) number of queries per user of the ESP profile;	(a) number of queries per user of the ESP profile;	(a) number of queries per user of the ESP profile;	
884	(b) number of queries to each of the Interpol databases.	(b) number of queries to each of the Interpol databases.	(b) number of queries to each of the Interpol databases.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
885	2. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the common identity repository, solely for the purposes of reporting and statistics without enabling individual identification:	2. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the common identity repository, solely for the purposes of reporting and statistics without enabling individual . <i>The use of these data shall not allow for the identification of a person:</i>	2. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the common identity repository (<i>CIR</i>), solely for the purposes of reporting and statistics without enabling individual identification:	
886	(a) number of queries for the purposes of Articles 20, 21 and 22;	(a) number of queries for the purposes of Articles 20, 21 and 22;	(a) number of queries for the purposes of Articles 20, 21 and 22;	
887	(b) nationality, sex and year of birth of the person;	(b) nationality, sex and year of birth of the person;	(b) nationality, sex <i>gender</i> and year of birth of the person;	
888	(c) the type of the travel document and the three-letter code of the issuing country;	(c) the type of the travel document and the three-letter code of the issuing country;	(c) the type of the travel document and the three-letter code of the issuing country;	
889	(d) the number of searches conducted with and without biometric data.	(d) the number of searches conducted with and without biometric data.	(d) the number of searches conducted with and without biometric data.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
890	3. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the multiple-identity detector, solely for the purposes of reporting and statistics without enabling individual identification:	3. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the multiple-identity detector, solely for the purposes of reporting and statistics without enabling individual . <i>The use of these data shall not allow for the identification of a person:</i>	3. The duly authorised staff of the competent authorities of Member States, the Commission and eu-LISA shall have access to consult the following data related to the multiple-identity detector (<i>MID</i>), solely for the purposes of reporting and statistics without enabling individual identification:	
891	(a) nationality, sex and year of birth of the person;	(a) nationality, sex and year of birth of the person;	(a) — nationality, sex and year of birth of the person;	
892	(a) the type of the travel document and the three-letter code of the issuing country;	(a) the type of the travel document and the three-letter code of the issuing country;	(a) — the type of the travel document and the three letter code of the issuing country;	
893	(b) the number of searches conducted with and without biometric data;	(b) the number of searches conducted with and without biometric data;	(c) the number of searches conducted with and without biometric data;	
894	(c) the number of each type of link.	(c) the number of each type of link.	(d) the number of each type of link <i>and the EU information systems between which each link was established;-</i>	
895		<i>(da) the number of linkages between the various Union</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>information systems;</i>		
896		<i>(db) the period of time for which a yellow link remained in the system;</i>		
897		<i>(dc) the period of time for which a red link remained in the system.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
898			<i>(e) the period of time a yellow link or a red link remained.</i>	
899	4. The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council ¹⁰⁸ shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.	4. The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council ¹⁰⁹ shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.	4. The duly authorised staff of the European Border and Coast Guard Agency established by Regulation (EU) 2016/1624 of the European Parliament and of the Council ¹¹⁰ shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out risk analyses and vulnerability assessments as referred to in Articles 11 and 13 of that Regulation.	

¹⁰⁸ Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

¹⁰⁹ Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

¹¹⁰ Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC (OJ L 251, 16.9.2016, p. 1).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
900			<i>4a. The duly authorised staff of Europol shall have access to consult the data referred to in paragraphs 1, 2 and 3 for the purpose of carrying out strategic, thematic and operational analyses as referred to in Article 18(2)(b) and (c) of Regulation (EU) 2016/794.</i>	
901	5. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 of this Article in the central repository for reporting and statistics referred to in Chapter VII of this Regulation. The data included in the repository shall not enable the identification of individuals, but it shall allow the authorities listed in paragraph 1 of this Article to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policymaking on	5. For the purpose of paragraph 1 of this Article, eu-LISA shall store the data referred to in paragraph 1 of this Article in the central repository for reporting and statistics referred to in Chapter VII of this Regulation. The data included in the repository shall not enable the identification of individuals, but it shall allow the authorities listed in paragraph 1 of this Article to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based policymaking on	5. For the purpose of paragraphs 1, 2 and 3 of this Article, eu-LISA shall store the data referred to in paragraph 1 of this Article in the central repository for reporting and statistics referred to in Chapter VII of this Regulation. The data included in the repository shall not enable the identification of individuals, but it shall allow the authorities listed in paragraph 1 of this Article to obtain customisable reports and statistics to enhance the efficiency of border checks, to help authorities processing visa applications and to support evidence-based	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	migration and security in the Union.	migration and security in the Union.	policymaking on migration and security in the Union.	
902		<i>5a. Meaningful summaries shall be made available to the Agency for Fundamental Rights in order to evaluate the impact on fundamental rights of this Regulation.</i>		
903	<i>Article 57 Transitional period for the use of the European search portal</i>	<i>Article 57 Transitional period for the use of the European search portal</i>	<i>Article 57 Transitional period for the use of the European search portal</i>	
904	For a period of two years from the date the ESP commences operations, the obligations referred to in Article 7(2) and (4) shall not apply and the utilisation of the ESP shall be optional.	For a period of two years from the date the ESP commences operations, the obligations referred to in Article 7(2) and (4) shall not apply and the utilisation of the ESP shall be optional.	1. For a period of two years from the date the ESP commences operations, the obligations referred to in Article 7(2) and (4) shall not apply and the utilisation of the ESP shall be optional.	
905			2. <i>Following the period referred to in paragraph 1, the Commission, in close cooperation with Member States and eu-LISA, shall assess the impact of the ESP on border checks. On the basis of this assessment, and after consultation with the Member</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>States, the Commission may adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1 until any potential technical issue linked to the ESP has been solved.</i>	
906	<i>Article 58 Transitional period applicable to the provisions on access to the common identity repository for law enforcement purposes</i>	<i>Article 58 Transitional period applicable to the provisions on access to the common identity repository for law enforcement purposes</i>	<i>Article 58 Transitional period applicable to the provisions on access to the common identity repository for law enforcement purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences</i>	
907	Article 22, points 13, 14, 15 and 16 of Article 55b and Article 55e shall apply from the date of the start of operations referred to in Article 62(1).	Article 22, points 13, 14, 15 and 16 of Article 55b and Article 55e shall apply from the date of the start of operations referred to in Article 62(1).	Article 22, points 13, 14, 15, 16 and 16a of Article 55b, and Article 55e and points 14 and 15 of Article 15f shall apply from the date of the start of operations referred to in Article 62(1).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
908	<i>Article 59 Transitional period for the multiple-identity detection</i>	<i>Article 59 Transitional period for the multiple-identity detection</i>	<i>Article 59 Transitional period for the multiple-identity detection</i>	
909	1. For a period of one year following the notification by eu-LISA of the completion of the test referred to in Article 62(1)(b) regarding the multiple-identity detector (MID) and before the start of operations of the MID, the ETIAS Central Unit as referred to in [Article 33(a) of Regulation (EU) 2016/1624] shall be responsible for carrying out a multiple-identity detection between the data stored in the VIS, Eurodac and the SIS. The multiple-identity detections shall be carried out using only biometric data in accordance with Article 27(2) of this Regulation.	1. For a period of one year following the notification by eu-LISA of the completion of the test referred to in Article 62(1)(b) regarding the multiple-identity detector (MID) and before the start of operations of the MID, the ETIAS Central Unit as referred to in [Article 33(a) of Regulation (EU) 2016/1624] shall be responsible for carrying out a multiple-identity detection between the data stored in the VIS, Eurodac, and the the EES and SIS. The multiple-identity detections shall be carried out using only biometric data in accordance with Article 27(2) of this Regulation.	1. For a period of one year following the notification by eu-LISA of the completion of the test referred to in Article 62(1)(b) regarding the multiple-identity detector (MID) and before the start of operations of the MID, the ETIAS Central Unit as referred to in [Article 33(a) of Regulation (EU) 2016/1624] shall be responsible for carrying out a multiple-identity detection between the data stored in the EES , VIS, Eurodac and the SIS. The multiple-identity detections shall be carried out using only biometric data in accordance with Article 27(2) of this Regulation.	
910		1a. Following the period referred to in paragraph 1, the Commission shall, in close cooperation with the ETIAS Central Unit, create a network of		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>liaison officers to be hosted in the ETIAS Central Unit or single points of contact of the competent Member States' authorities for the performance of the task laid down in this Article.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
911	2. Where the query reports one or several hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.	2. Where the query reports one or several hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.	2. Where the query reports one or several <i>match(es)</i> hit(s) and the identity data of the linked files is identical or similar, a white link shall be created in accordance with Article 33.	
912	Where the query reports one or several hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.	Where the query reports one or several hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.	Where the query reports one or several <i>match(es)</i> hit(s) and the identity data of the linked files cannot be considered as similar, a yellow link shall be created in accordance with Article 30 and the procedure referred to in Article 29 shall apply.	
913	Where several hits are reported, a link shall be created to each piece of data triggering the hit.	Where several hits are reported, a link shall be created to each piece of data triggering the hit.	Where several hits <i>matches</i> are reported, a link shall be created to each piece of data triggering the hit <i>match</i> .	
914	3. Where a yellow link is created, the MID shall grant access to the identity data present in the different information systems to the ETIAS Central Unit.	3. Where a yellow link is created, the MID shall grant access to the identity data present in the different information systems to the ETIAS Central Unit.	3. Where a yellow link is created, the MID shall grant access to the identity data present in the different information systems to the ETIAS Central Unit.	

	<p style="text-align: center;">Amended Commission proposal (ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate (ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>915</p>	<p>4. Where a link is created to an alert in the SIS, other than a refusal of entry alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Article 24 of the Regulation on SIS in the field of border checks and Article 38 of the Regulation on SIS in the field of law enforcement respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.</p>	<p>4. Where a link is created to an alert in the SIS, other than a refusal of entry alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Article 24 of the Regulation on SIS in the field of border checks and Article 38 of the Regulation on SIS in the field of law enforcement respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.</p>	<p>4. Where a link is created to an alert in the SIS, other than a refusal of entry <i>or return</i> alert or an alert on a travel document reported lost, stolen or invalidated in accordance with Articles 24 <i>and 25</i> of the Regulation on SIS in the field of border checks, <i>Article 3 of the Regulation on the use of SIS for the return of illegally staying third-country nationals</i> and Article 38 of the Regulation on SIS in the field of law enforcement <i>police cooperation and judicial cooperation in criminal matters</i> respectively, the MID shall grant access to the identity data present in the different information systems to the SIRENE Bureau of the Member State that created the alert.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
916	5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file.	5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file.	5. The ETIAS Central Unit or the SIRENE Bureau of the Member State that created the alert shall have access to the data contained in the identity confirmation file and shall assess the different identities and shall update the link in accordance with Articles 31, 32 and 33 and add it to the identity confirmation file.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
917		<i>5a. Notification under Article 61(3) shall only be made once all yellow links have been verified and changed either into a green or into a red link.</i>		
918	6. eu-LISA shall assist where necessary the ETIAS Central Unit in carrying out the multiple-identity detection referred to in this Article.	6. eu-LISA shall assist where necessary the ETIAS Central Unit in carrying out the multiple-identity detection referred to in this Article.	6. eu-LISA Member States shall assist where necessary the ETIAS Central Unit in carrying out the multiple-identity detection referred to in this Article.	
919			<i>7. Where a red link is created between data in the CIR, the identity confirmation file including the red link shall be stored in the MID at least for three years or for as long as the corresponding data are stored in at least one of the EU information systems.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
920			<i>8. Where a red link is created between data in the CIR, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR at least for three years or for as long as the corresponding data are stored in at least one of the EU information systems.</i>	
921			<i>9. Where a red link is created between data in the CIR and the SIS, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR for as long as the corresponding data are stored in the SIS.</i>	
922			<i>10. Following the period referred to in paragraph 1, the Commission, in close cooperation with Member States and the ETIAS Central Unit, shall assess the need to extend the transitional period in which the ETIAS Central Unit performs the tasks referred to in this Article. On the basis of this</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			<i>assessment, and after consultation with the Member States, the Commission may adopt a delegated act in accordance with Article 63 to extend the period referred to in paragraph 1.</i>	
923	<i>Article 60 Costs</i>	<i>Article 60 Costs</i>	<i>Article 60 Costs</i>	
924	1. The costs incurred in connection with the establishment and operation of the ESP, the shared biometric matching service, the common identity repository (CIR) and the MID shall be borne by the general budget of the Union.	1. The costs incurred in connection with the establishment and operation of the ESP, the shared biometric matching service, the common identity repository (CIR) and the MID shall be borne by the general budget of the Union.	1. The costs incurred in connection with the establishment and operation of the ESP, the shared biometric matching service (BMS), the common identity repository (CIR) and the MID shall be borne by the general budget of the Union.	
925		<i>1a. The cost incurred in connection with the establishment and operation of a central Union backup solution for each system indicated in paragraph 1, where necessary, shall be borne by the general budget of the Union.</i>		
926	2. Costs incurred in connection with the integration of	2. Costs incurred in connection with the integration of	2. Costs incurred in connection with the integration of	

	<p align="center">Amended Commission proposal (ST 10178/18)</p>	<p align="center">EP amendments</p>	<p align="center">Council negotiation mandate (ST 11312/18)</p>	<p align="center">Compromise text proposals</p>
	<p>the existing national infrastructures and their connection to the national uniform interfaces as well as in connection with hosting the national uniform interfaces shall be borne by the general budget of the Union.</p>	<p>the existing national infrastructures and their connection to the national uniform interfaces as well as in connection with hosting the national uniform interfaces shall be borne by the general budget of the Union.</p>	<p>the existing national infrastructures and their connection to the national uniform interfaces as well as in connection with hosting the national uniform interfaces shall be borne by the general budget of the Union.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
927	The following costs shall be excluded:	The following costs shall be excluded:	The following costs shall be excluded:	
928	(a) Member States' project management office (meetings, missions, offices);	(a) Member States' project management office (meetings, missions, offices);	(a) Member States' project management office (meetings, missions, offices);	
929	(b) hosting of national IT systems (space, implementation, electricity, cooling);	(b) hosting of national IT systems (space, implementation, electricity, cooling);	(b) hosting of national IT systems (space, implementation, electricity, cooling);	
930	(c) operation of national IT systems (operators and support contracts);	(c) operation of national IT systems (operators and support contracts);	(c) operation of national IT systems (operators and support contracts);	
931	(d) design, development, implementation, operation and maintenance of national communication networks.	(d) design, development, implementation, operation and maintenance of national communication networks.	(d) design, development, implementation, operation and maintenance of national communication networks.	
932	3. The costs incurred by the designated authorities referred to in Article 4(24) shall be borne, respectively, by each Member State and Europol. The costs for the connection of the designated authorities to the CIR shall be borne by each Member State and Europol,	3. The costs incurred by the designated authorities referred to in Article 4(24) shall be borne, respectively, by each Member State and Europol. The costs for the connection of the designated authorities to the CIR shall be borne by each Member State and Europol,	3. The costs incurred by the designated authorities referred to in Article 4(24) shall be borne, respectively, by each Member State and Europol. The costs for the connection of the designated authorities to the CIR shall be borne by each Member State and Europol,	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	respectively.	respectively.	respectively.	
933	<i>Article 61 Notifications</i>	<i>Article 61 Notifications</i>	<i>Article 61 Notifications</i>	
934	1. The Member States shall notify eu-LISA of the authorities referred to in Articles 7, 20, 21 and 26 that may use or have access to the ESP, the CIR and the MID respectively.	1. The Member States shall notify eu-LISA of the authorities referred to in Articles 7, 20, 21 and 26 that may use or have access to the ESP, the CIR and the MID respectively.	1. The Member States shall notify eu-LISA of the authorities referred to in Articles 7, 20, 21 and 26 that may use or have access to the ESP, the CIR and the MID respectively.	
935	A consolidated list of those authorities shall be published in the <i>Official Journal of the European Union</i> within a period of three months from the date on which each interoperability component commenced operations in accordance with Article 62. Where there are amendments to the list, eu-LISA shall publish an updated consolidated list once a year.	A consolidated list of those authorities shall be published in the <i>Official Journal of the European Union</i> within a period of three months from the date on which each interoperability component commenced operations in accordance with Article 62. Where there are amendments to the list, eu-LISA shall publish an updated consolidated list once a year. <i>The list shall include the date of notification for each authority listed.</i>	A consolidated list of those authorities shall be published in the <i>Official Journal of the European Union</i> within a period of three months from the date on which each interoperability component commenced operations in accordance with Article 62. Where there are amendments to the list, eu-LISA shall publish an updated consolidated list once a year.	
936	2. eu-LISA shall notify the Commission of the successful	2. eu-LISA shall notify the Commission of the successful	2. eu-LISA shall notify the Commission of the successful	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	completion of the test referred to in Article 62(1)(b).	completion of the test referred to in Article 62(1)(b).	completion of the test referred to in Article 62(1)(b).	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
937	3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional measure laid down in Article 59.	3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional measure laid down in Article 59.	3. The ETIAS Central Unit shall notify the Commission of the successful completion of the transitional measure laid down in Article 59.	
938	4. The Commission shall make available to the Member States and the public, by a constantly updated public website, the information notified pursuant to paragraph 1.	4. The Commission shall make available to the Member States and the public, by a constantly updated public website, the information notified pursuant to paragraph 1.	4. The Commission shall make available to the Member States and the public, by a constantly updated public website, the information notified pursuant to paragraph 1.	
939	<i>Article 62 Start of operations</i>	<i>Article 62 Start of operations</i>	<i>Article 62 Start of operations</i>	
940	1. The Commission shall decide the date from which each interoperability component is to start operations, after the following conditions are met:	1. <i>No later than five years after the entry into force of this Regulation</i> , the Commission shall decide <i>adopt a decision setting</i> the date from <i>on</i> which each interoperability component is to start operations, after the following conditions are met:	1. The Commission shall decide the date from which each interoperability component is to start operations, after the following conditions are met:	
941	(a) the measures referred to in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5) have been adopted;	(a) the measures referred to in Articles 8(2), 9(7), 28(5) and (6), 37(4), 38(4), 39(5) and 44(5) have been adopted;	(a) the measures referred to in Articles 8(2), 9(7), <i>13(5)</i> , 28(5), <i>(5a)</i> and <i>(7c)</i> , <i>32(4a)</i> , <i>33(4a)</i> , 37(4), 38(4), 39(5), and	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
			44(5), 57(2) and 59(10), 68(7a) have been adopted;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
942	(b) eu-LISA has declared the successful completion of a comprehensive test of the relevant interoperability component, which is to be conducted by eu-LISA in cooperation with the Member States;	(b) eu-LISA has declared the successful completion of a comprehensive test of the relevant interoperability component, which is to be conducted by eu-LISA in cooperation with the Member States, <i>the ETIAS Central Unit and Europol</i> ;	(b) eu-LISA has declared the successful completion of a comprehensive test of the relevant interoperability component, which is to be conducted by eu-LISA in cooperation with the Member States, <i>the ETIAS Central Unit and Europol</i> ;	
943	(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Articles 8(1), 13, 19, 34 and 39 and have notified them to the Commission;	(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Articles 8(1), 13, 19, 34 and 39 and have notified them to the Commission;	(c) eu-LISA has validated the technical and legal arrangements to collect and transmit the data referred to in Articles 8(1), 13, 19 18 , 34 and 39 and have has notified them to the Commission;	
944	(d) the Member States have notified the Commission as referred to in Article 61(1);	(d) the Member States have notified the Commission as referred to in Article 61(1);	(d) the Member States have notified the Commission as referred to in Article 61(1);	
945	(e) for the multiple-identity detector, the ETIAS Central Unit has notified the Commission as referred to in Article 61(3).	(e) for the multiple-identity detector, the ETIAS Central Unit has notified the Commission as referred to in Article 61(3).	(e) for the multiple-identity detector, the ETIAS Central Unit has notified the Commission as referred to in Article 61(3).	
946		<i>The date referred to in the first subparagraph shall be set for within 30 days from the decision</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>of the Commission.</i>		
947		<i>1a. By way of derogation from paragraph 1, the measures referred to in Article 37 shall apply as of ... [one year after the entry into force of this Regulation].</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
948	2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraph 1(b).	2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraph 1(b).	2. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to paragraph 1(b).	
949	3. The Commission decision referred to in paragraph 1 shall be published in the <i>Official Journal of the European Union</i> .	3. The Commission decision referred to in paragraph 1 shall be published in the <i>Official Journal of the European Union</i> .	3. The Commission decision referred to in paragraph 1 shall be published in the <i>Official Journal of the European Union</i> .	
950	4. The Member States and Europol shall start using the interoperability components from the date determined by the Commission in accordance with paragraph 1.	4. The Member States and Europol shall start using the interoperability components from the date determined by the Commission in accordance with paragraph 1.	4. The Member States, <i>the ETIAS Central Unit</i> and Europol shall start using the interoperability components from the date determined by the Commission in accordance with paragraph 1.	
951	<i>Article 63 Exercise of the delegation</i>	<i>Article 63 Exercise of the delegation</i>	<i>Article 63 Exercise of the delegation</i>	
952	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
953	2. The power to adopt delegated acts referred to in Articles 8(2) and 9(7) shall be conferred on the Commission for an indeterminate period of time from [<i>the date of entry into force of this Regulation</i>].	2. The power to adopt delegated acts referred to in Articles 8(2), and 9(7) , 28(5) and 39(5) shall be conferred on the Commission for an indeterminate period of time from [the date of entry into force of this Regulation].	2. The power to adopt delegated acts referred to in Articles 8(2), and 9(7) 57(2) and 59(10) shall be conferred on the Commission for an indeterminate a period of five years time from [<i>the date of entry into force of this Regulation</i>]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
954	3. The delegation of power referred to in Articles 8(2) and 9(7) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in Articles 8(2), and 9(7) , 28(5) and 39(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in Articles 8(2) and 9(7) 57(2) and 59(10) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	
955	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
956	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	
957	6. A delegated act adopted pursuant to Articles 8(2) and 9(7) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.	6. A delegated act adopted pursuant to Articles 8(2), and 9(7) , 28(5) and 39(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.	6. A delegated act adopted pursuant to Articles 8(2) and 9(7) 57(2) and 59(10) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
958	<i>Article 64 Committee procedure</i>	<i>Article 64 Committee procedure</i>	<i>Article 64 Committee procedure</i>	
959	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	
960	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. <i>Where the Committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.</i>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
961	<i>Article 65 Advisory group</i>	<i>Article 65 Advisory group</i>	<i>Article 65 Advisory group</i>	
962	An Advisory Group shall be established by eu-LISA in order to provide it with the expertise related to interoperability, in particular in the context of the preparation of its annual work programme and its annual activity report. During the design and development phase of the interoperability instruments, Article 52(4) to (6) shall apply.	An Advisory Group shall be established by eu-LISA in order to provide it with the expertise related to interoperability, in particular in the context of the preparation of its annual work programme and its annual activity report. During the design and development phase of the interoperability instruments, Article 52(4) to (6) shall apply.	An Advisory Group shall be established by eu-LISA in order to provide it with the expertise related to interoperability, in particular in the context of the preparation of its annual work programme and its annual activity report. During the design and development phase of the interoperability instruments, Article 52(4) to (6) shall apply.	
963	<i>Article 66 Training</i>	<i>Article 66 Training</i>	<i>Article 66 Training</i>	
964	eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) No 1077/2011.	eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) No 1077/2011.	I. eu-LISA shall perform tasks related to the provision of training on the technical use of the interoperability components in accordance with Regulation (EU) No 1077/2011.	
965		<i>Member States and Union agencies shall organise for their staff authorised to process data from the interoperability</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>components, appropriate training programme about data security, data quality, data protection rules and the procedures of the data processing.</i>		
966		<i>Common training courses on data security, data quality, data protection rules and the procedures for data processing shall be organised at Union level at least once a year to enhance cooperation and exchange of best practices between staff of Member States and Union bodies which are authorised to process data from the interoperability components.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
967			2. <i>The staff of Member State authorities, [the ETIAS Central Unit] and Europol, authorised to process data from the interoperability components, shall receive appropriate training about data security, data protection rules and the procedures of data processing, in which particular attention is paid to the process of multiple identity detection, including the verification of links and the accompanying need to ensure the safeguards in relation to fundamental rights.</i>	
968	<i>Article 67 Practical handbook</i>	<i>Article 67 Practical handbook</i>	<i>Article 67 Practical handbook</i>	
969	The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant agencies, make available a practical handbook for the implementation and management of the interoperability components. The practical handbook shall provide	The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant agencies, <i>update the practical handbooks made available for the EES, VIS, [ETIAS], Eurodac, SIS and [ECRIS-TCN] with information necessary and</i> make available a	The Commission shall, in close cooperation with the Member States, eu-LISA and other relevant agencies, make available a practical handbook for the implementation and management of the interoperability components. The practical handbook shall provide	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation.	practical handbook for the implementation and management of the interoperability components. The practical handbook handbooks shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the <i>updates in accordance with the rules and in the form laid down in the respective legal instruments. The practical handbook on the interoperability components shall be adopted</i> in the form of a recommendation.	technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation.	
970		<i>The practical handbook should provide guidance to Member States on how to deal with yellow links that are the results of inconsistencies with the identity data contained in ETIAS. Such modalities should not create disproportionate burdens on persons who, without any intention to deceive the authorities, have entered</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>inaccurate or ambiguous data in ETIAS.</i>		
971	<i>Article 68 Monitoring and evaluation</i>	<i>Article 68 Monitoring and evaluation</i>	<i>Article 68 Monitoring and evaluation</i>	
972	1. eu-LISA shall ensure that procedures are in place to monitor the development of the interoperability components in light of objectives relating to planning and costs and to monitor the functioning of the interoperability components in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.	1. eu-LISA shall ensure that procedures are in place to monitor the development of the interoperability components and the integration of the existing national infrastructure and connection to the national uniform interface in light of objectives relating to planning and costs and to monitor the functioning of the interoperability components in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.	1. eu-LISA shall ensure that procedures are in place to monitor the development of the interoperability components in light of objectives relating to planning and costs and to monitor the functioning of the interoperability components in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.	

	<p style="text-align: center;">Amended Commission proposal</p> <p style="text-align: center;">(ST 10178/18)</p>	<p style="text-align: center;">EP amendments</p>	<p style="text-align: center;">Council negotiation mandate</p> <p style="text-align: center;">(ST 11312/18)</p>	<p style="text-align: center;">Compromise text proposals</p>
<p>973</p>	<p>2. By [<i>Six months after the entry into force of this Regulation</i> — OPOCE, please replace with the actual date] and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the interoperability components. Once the development is finalised, a report shall be submitted to the European Parliament and the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.</p>	<p>2. By [Six months after the entry into force of this Regulation — OPOCE, please replace with the actual date] and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the interoperability components. Once the development is finalised, a <i>That</i> report shall be submitted to the European Parliament and the Council explaining in detail how the objectives, in particular relating to planning and <i>include an overview of the current development of costs and progress of the project, a financial impact assessment, and information on any technical problems and risks that may impact the overall</i> costs, were achieved as well as justifying any divergences <i>of the system to be</i></p>	<p>2. By [<i>Six months after the entry into force of this Regulation</i> — OPOCE, please replace with the actual date] and every six months thereafter during the development phase of the interoperability components, eu-LISA shall submit a report to the European Parliament and the Council on the state of play of the development of the interoperability components. Once the development is finalised, a report shall be submitted to the European Parliament and the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved as well as justifying any divergences.</p>	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>borne by the general budget of the Union in accordance with Article 60.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
974		<i>2a. Six months after the start of the operations of each interoperability component, eu-LISA shall submit a report to the European Parliament and to the Council on the state of play of the connection by Member States to the communication infrastructure of the ESP and the CIR and the integration of the existing national systems and infrastructure with the ESP, shared BMS, the MID and the CIR.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
975		<i>2b. In the event of delays in the development process, the European Parliament and the Council shall be informed by eu-LISA as soon as possible of the reasons for the delays and of their impact in terms of time and finances.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
976		<i>2c. During the development phase of the interoperability components, the Commission shall evaluate the necessity of further harmonisation of the national systems and infrastructure of Member States at the external borders. The Commission shall transmit the evaluation report to the European Parliament and to the Council. These evaluation reports shall include recommendations, an impact assessment and an assessment of the cost for the Union budget.</i>		
977	3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the interoperability components.	3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the interoperability components <i>without having access to any personal data processed by those components. Such access shall be logged.</i>	3. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the interoperability components.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
978	4. Four years after the start of operations of each interoperability component and every four years thereafter, eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the interoperability components, including the security thereof.	4. Four Three years after the start of operations of each interoperability component and every four three years thereafter, eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the connection of Member States to the communication infrastructure of the ESP and the CIR and the integration of the existing national systems and infrastructure with the ESP, shared BMS, the MID and the CIR, as well as on the technical functioning of the interoperability components, including the security thereof.	4. Four years after the start of operations of each interoperability component and every four years thereafter, eu-LISA shall submit to the European Parliament, the Council and the Commission a report on the technical functioning of the interoperability components, including the security thereof.	
979	5. In addition, one year after each report from eu-LISA, the Commission shall produce an overall evaluation of the components, including:	5. In addition, one year after each report from eu-LISA, the Commission shall produce an overall evaluation of the components, including:	5. In addition, one year after each report from eu-LISA, the Commission shall produce an overall evaluation of the components, including:	
980	(a) an assessment of the application of this Regulation;	(a) an assessment of the application of this Regulation;	(a) an assessment of the application of this Regulation;	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
981	(b) an examination of the results achieved against objectives and the impact on fundamental rights;	(b) an examination of the results achieved against objectives and the impact on fundamental rights;	(b) an examination of the results achieved against objectives and the impact on fundamental rights;	
982	(c) an assessment of the continuing validity of the underlying rationale of the interoperability components;	(c) an assessment of the continuing validity of the underlying rationale of the interoperability components;	(c) an assessment of the continuing validity of the underlying rationale of the interoperability components;	
983	(d) an assessment of the security of the interoperability components;	(d) an assessment of the security of the interoperability components;	(d) an assessment of the security of the interoperability components;	
984		<i>(da) an assessment of the Member States' use of the CIR for identification;</i>		
985		<i>(db) an assessment to ensure that Member States are in full compliance with their obligations with respect to each Union information system;</i>		
986		<i>(dc) an assessment of the security of Member States' connection to the communication infrastructure of the ESP and the CIR and the security of the integration of the</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>existing national systems and infrastructure with the ESP, shared BMS, the MID and the CIR;</i>		
987		<i>(dd) an assessment of queries of the CIR for law enforcement purposes;</i>		
988	(e) an assessment of any implications, including any disproportionate impact on the flow of traffic at border crossing points and those with a budgetary impact on the Union budget.	(e) an assessment of any implications, including any disproportionate impact on the flow of traffic at border crossing points and those with a budgetary impact on the Union budget.	(e) an assessment of any implications, including any disproportionate impact on the flow of traffic at border crossing points and those with a budgetary impact on the Union budget.	
989		<i>(ea) an assessment of the search of the Interpol databases via the ESP, including information on the number of hits against Interpol databases and information on any problems encountered.</i>		
990	The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data	The evaluations shall include any necessary recommendations. The Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data	The evaluations shall include any necessary recommendations, <i>including the possibility, if appropriate, to conduct parallel searches in different EU information systems.</i> The	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
	Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007. ¹¹¹	Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007. ¹¹²	Commission shall transmit the evaluation report to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007. ¹¹³	
991	6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.	6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.	6. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 4 and 5. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.	

¹¹¹ Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

¹¹² Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

¹¹³ Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
992	7. eu-LISA shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.	7. eu-LISA shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.	7. eu-LISA shall provide the Commission with the information necessary to produce the evaluations referred to in paragraph 5.	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
993			<i>7a. A technical solution shall be made available to Member States in order to facilitate the querying of EU information systems and the CIR pursuant to Article 22 for the purpose of managing users request and generating statistics referred to in this Article. The Commission shall adopt implementing acts concerning the specifications of the technical solution. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 64(2).</i>	
994	8. While respecting the provisions of national law on the publication of sensitive information, each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the common identity repository for law enforcement purposes, containing information and statistics on:	While respecting the provisions of national law on the publication of sensitive information <i>including limitations deriving from matters of national security</i> , each Member State and Europol shall prepare annual reports on the effectiveness of access to data stored in the common identity repository for law enforcement purposes,	8. While respecting the provisions of national law on the publication of sensitive information, <i>and without prejudice to limitations necessary to protect security and public order, prevent crime and guarantee that any national investigation will not be jeopardised</i> , each Member State and Europol shall prepare annual	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		containing information and statistics on:	reports on the effectiveness of access to data stored in the common identity repository for law enforcement purposes <i>of preventing, detecting or investigation terrorist offences or other serious criminal offences</i> , containing information and statistics on:	
995	(a) the exact purpose of the consultation including the type of terrorist or serious criminal offence;	(a) the exact purpose of the consultation including the type of terrorist or serious criminal offence;	(a) the exact purpose of the consultation including the type of terrorist or serious criminal offence;	
996	(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by the [EES Regulation], the VIS Regulation or the [ETIAS Regulation];	(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by the [EES Regulation], the VIS Regulation or the [ETIAS Regulation];	(b) reasonable grounds given for the substantiated suspicion that the suspect, perpetrator or victim is covered by the [EES Regulation] Regulation (EU) 2017/2226 , the VIS Regulation (EC) No 767/2008 or the [ETIAS Regulation];	

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
997	(c) the number of requests for access to the common identity repository for law enforcement purposes;	(c) the number of requests for access to the common identity repository for law enforcement purposes;	(c) the number of requests for access to the CIR common identity repository for law enforcement purposes <i>of preventing, detecting or investigating terrorist offences or other serious criminal offences</i> ;	
998	(d) the number and type of cases that have ended in successful identifications;	(d) the number and type of cases that have ended in successful identifications;	(d) the number and type of cases that have ended in successful identifications;	
999	(e) the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the <i>ex post</i> verification carried out by the central access point.	(e) the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the <i>ex post</i> verification carried out by the central access point.	(e) the need and use made of the exceptional case of urgency including those cases where that urgency was not accepted by the <i>ex post</i> verification carried out by the central access point.	
100	Member State and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.	Member State and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.	Member State and Europol annual reports shall be transmitted to the Commission by 30 June of the subsequent year.	
100		<i>The Commission shall transmit those reports to the European Parliament, to the Council, to the European Data Protection</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
		<i>Supervisor and to the European Union Agency for Fundamental Rights.</i>		

	Amended Commission proposal (ST 10178/18)	EP amendments	Council negotiation mandate (ST 11312/18)	Compromise text proposals
100	<i>Article 69 Entry into force and applicability</i>	<i>Article 69 Entry into force and applicability</i>	<i>Article 69 Entry into force and applicability</i>	
100	This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i> .	This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i> .	This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i> .	
100	This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.	This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.	This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.	
100	Done at Strasbourg, <i>For the European Parliament</i> The President <i>For the Council</i> The President	Done at Strasbourg, <i>For the European Parliament</i> The President <i>For the Council</i> The President	Done at Strasbourg, <i>For the European Parliament</i> The President <i>For the Council</i> The President	