LIBE comments in green. Presidency comments in turquoise. Provisionally agreed.

18 April 2018

Proposal for a

REGULATION 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

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
1	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 Articles 82(1) second subparagraph point (d), 85(1), 87(2)(a) and 88(2)(a) thereof,		Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 82(1) second subparagraph point (d), 85(1), 87(2)(a) and 88(2)(a) thereof,	
3	Having regard to the proposal from the European Commission,		Having regard to the proposal from the European Commission,	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
4	After transmission of the draft legislative act to the national parliaments,		After transmission of the draft legislative act to the national parliaments,	
5	Acting in accordance with the ordinary legislative procedure,		Acting in accordance with the ordinary legislative procedure,	
6	Whereas:		Whereas:	
7	(1) The Schengen information system (SIS) constitutes an essential tool for the application of the provisions of the Schengen acquis as integrated into the framework of the European Union. SIS is one of the major compensatory measures contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between border guards, police, customs and other law enforcement and judicial authorities in criminal matters.		(1) The Schengen information system (SIS) constitutes an essential tool for the application of the provisions of the Schengen acquis as integrated into the framework of the European Union. SIS is one of the major compensatory measures **and law enforcement tools** contributing to maintaining a high level of security within the area of freedom, security and justice of the European Union by supporting operational cooperation between border guards, police, customs and other ~~law enforcement and judicial~~ authorities **responsible for the prevention, the detection, investigation or prosecution of criminal ofences or the execution of** ~~in~~ criminal **penalties and**	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			checks on third-country nationals~~matters~~[1].	
8	(2) SIS was set up pursuant to the provisions of Title IV of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders[2] (the Schengen Convention). The development of the second generation of SIS (SIS II) was entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001[3] and Council Decision 2001/886/JHA[4] and it was established by Regulation (EC) No 1987/2006[5] as well as by Council Decision 2007/533/JHA[6]. SIS II replaced SIS as created		(2) SIS was **initially** set up pursuant to the provisions of Title IV of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders[2] (the Schengen Convention). The development of the second generation of SIS (SIS II) was entrusted to the Commission pursuant to Council Regulation (EC) No 2424/2001[3] and Council Decision 2001/886/JHA[4] and it was established by Regulation (EC) No 1987/2006[5] as well as by Council Decision 2007/533/JHA[6]. SIS II replaced SIS as created	

1 Wording in line with Article 43(1)(c).
2 OJ L 239, 22.9.2000, p. 19. Convention as amended by Regulation (EC) No 1160/2005 of the European Parliament and of the Council (OJ L 191, 22.7.2005, p. 18).
3 OJ L 328, 13.12.2001, p. 4.
4 Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II) (OJ L 328, 13.12.2001, p. 1).
5 Regulation (EC) No 1987/2006 of 20 December 2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information system (SIS II) (OJ L181, 28.12.2006, p. 4).
6 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).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	pursuant to the Schengen Convention.		pursuant to the Schengen Convention.	
9	(3) Three years after SIS II was brought into operation, the Commission carried out an evaluation of the system in accordance with Articles 24(5), 43(5) and 50(5) of Regulation (EC) No 1987/2006 and Articles 59 and 65(5) of Decision 2007/533/JHA. The evaluation report and the related Staff Working Document were adopted on 21 December 2016[7]. The recommendations set out in those documents should be reflected, as appropriate, in this Regulation.		(3) Three years after SIS II was brought into operation, the Commission carried out an evaluation of the system in accordance with Articles 24(5), 43(5) and 50(5) of Regulation (EC) No 1987/2006 and Articles 59 and 65(5) of Decision 2007/533/JHA. The evaluation report and the related Staff Working Document were adopted on 21 December 2016[7]. The recommendations set out in those documents **are** ~~should be~~ reflected, as appropriate, in this Regulation.	
10	(4) This Regulation constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of the Treaty on Functioning of the European Union. Regulation (EU) 2018/… of the European Parliament and of the Council on the establishment, operation and		(4) This Regulation constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapters 4 and 5 of Title V of the Treaty on Functioning of the European Union. Regulation (EU) 2018/… of the European Parliament and of the Council on the establishment, operation and	

[7] Report to the European Parliament and Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66(5) of Decision 2007/533/JHA and an accompanying Staff Working Document. (OJ…).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	use of the Schengen Information System (SIS) in the field of border checks[8] constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapter 2 of Title V of the Treaty on Functioning of the European Union.		use of the Schengen Information System (SIS) in the field of border checks[8] constitutes the necessary legislative basis for governing SIS in respect of matters falling within the scope of Chapter 2 of Title V of the Treaty on Functioning of the European Union.	
11	(5) The fact that the legislative basis necessary for governing SIS consists of separate instruments does not affect the principle that SIS constitutes one single information system that should operate as such. Certain provisions of these instruments should therefore be identical.	(5) The fact that the legislative basis necessary for governing SIS consists of separate instruments does not affect the principle that SIS constitutes one single information system that should operate as such. Certain provisions of these instruments should therefore be identical***, while other provisions should differ, in particular as regards the authorities authorised to access the data contained in SIS. The rules on the protection of personal data should be fully guaranteed, in particular the purpose limitation principle***.	(5) The fact that the legislative basis necessary for governing SIS consists of separate instruments does not affect the principle that SIS constitutes one single information system that should operate as such **and that should include a single network of SIRENE Bureaux for ensuring the exchange of supplementary information**. Certain provisions of these instruments should therefore be identical.	
12	(6) It is necessary to specify the objectives of SIS, its technical architecture and its financing, to lay down rules concerning its end-	(6) It is necessary to specify the objectives of SIS, its technical architecture and its financing, to lay down rules concerning its end-	(6) It is necessary to specify the objectives of SIS, **certain elements of** its technical architecture**,** ~~and~~ its financing, to	

[8] Regulation (EU) 2018/…

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	to-end operation and use and to define responsibilities, the categories of data to be entered into the system, the purposes for which the data are to be entered, the criteria for their entry, the authorities authorised to access the data, the use of biometric identifiers and further rules on data processing.	to-end operation and use and to define responsibilities, the categories of data to be entered into the system, the purposes for which the data are to be entered, the criteria for their entry, ***rules on the deletion of alerts,*** the authorities authorised to access the data, the use of biometric identifiers and further rules on ***data protection and*** data processing.	lay down rules concerning its end-to-end operation and use and to define responsibilities, the categories of data to be entered into the system, the purposes for which the data are to be entered **and processed**, the criteria for their entry, the authorities authorised to access the data, the use of biometric ~~identifiers~~**data** and further rules on data processing.	
13		***(6a) Competent authorities should be able to enter into SIS specific information relating to any specific, objective, physical characteristics of a person not subject to change. This information may relate to characteristics such as piercings, tattoos, marks, scars, etc. However, pursuant to Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council[9], the data entered into SIS should not reveal sensitive information about a person such as ethnicity, religion, disability, gender or sexual orientation.***		**New recital (6a) Text from point 1.1 SIRENE Manual** (2018-03-26) ***SIS should contain only the indispensable information allowing for the identification of a person or an object and the necessary action to be taken. In addition, Member States should exchange supplementary information related to the alert where required.***

[9] ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 20017 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).***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
14	(7) SIS includes a central system (Central SIS) and national systems with a full or partial copy of the SIS database. Considering that SIS is the most important information exchange instrument in Europe, it is necessary to ensure its uninterrupted operation at central as well as at national level. Therefore each Member State should establish a partial or full copy of the SIS database and should set up its backup system.	(7) SIS includes a central system (Central SIS) and national systems ***which may contain*** a full or partial copy of the SIS database. Considering that SIS is the most important information exchange instrument in Europe, it is necessary to ensure its uninterrupted operation at central as well as at national level. ***For this reason there should be a reliable common backup system of the Central SIS (an active-active solution) ensuring the continuous availability of SIS data to end-users in the event of a failure, upgrades or maintenance of the central system and a backup communication infrastructure. Considerable investments are needed to bolster and improve the central system, its backup systems and the communications infrastructure***.	(7) SIS includes a central system (Central SIS) and national systems **that may contain** ~~with~~ a full or partial copy of the SIS database **which may be shared by two or more Member States**. Considering that SIS is the most important information exchange instrument in Europe, **for ensuring security and an effective migration management,** it is necessary to ensure its uninterrupted operation at central as well as at national level. **The availability of the SIS should be subject to close monitoring at central and Member State level and any incident of unavailability for the end-users should be registered and reported to stakeholders at national and EU level.** ~~Therefore e~~**E**ach Member State should ~~establish a partial or full copy of the SIS database and should~~ set up **a** ~~its~~ backup **for its national** system. **Member States should also ensure uninterrupted connectivity with Central SIS by having duplicated, physically and geographically separated connection points. Central SIS**	*To be adapted in accordance with Art. 4.*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			should be operated to ensure its functioning 24 hours a day, 7 days a week. In order to achieve this, an active-active solution may be used.	
15			**(7A) The technical architecture of the SIS may be subject to change following technical developments while ensuring the highest degree of availability for end-users at central and national level, the fulfilment of all applicable data protection requirements, services necessary for the entry and processing of SIS data including searches in the SIS database as well as an encrypted virtual communication network dedicated to SIS data and the exchange of data between SIRENE Bureaux. The changes should be decided based upon an impact and cost assessment and will be communicated to the European Parliament and the Council.**	*To be adapted in accordance with Art. 4.*
16	(8) It is necessary to maintain a manual setting out the detailed rules for the exchange of certain supplementary information	(8) It is necessary to maintain a manual setting out the detailed rules for the exchange of certain supplementary information concerning the action called for by	(8) It is necessary to maintain a manual setting out the detailed rules for the exchange of ~~certain~~ supplementary information	*To be adapted in accordance with Art. 8(3a)/Art. 8(3)PC*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	concerning the action called for by alerts. National authorities in each Member State (the SIRENE Bureaux), should ensure the exchange of this information.	alerts ***(the SIRENE Manual)***. National authorities in each Member State (the SIRENE Bureaux), should ensure the exchange of this information ***in a fast and efficient manner***. ***In case of alerts on terrorism offences or on children the SIRENE Bureaux should act immediately.***	concerning the action called for by alerts. National authorities in each Member State (the SIRENE Bureaux), should ensure the exchange of this information.	
17	(9) In order to maintain the efficient exchange of supplementary information concerning the action to be taken specified in the alerts, it is appropriate to reinforce the functioning of the SIRENE Bureaux by specifying the requirements concerning the available resources, user training and the response time to the inquiries received from other SIRENE Bureaux.	(9) In order to ***ensure*** the efficient exchange of supplementary information concerning the action to be taken specified in the alerts, it is appropriate to reinforce the functioning of the SIRENE Bureaux by specifying the requirements concerning available resources, user training and the response time to the inquiries received from other SIRENE Bureaux.	(9) In order to maintain the efficient exchange of supplementary information ~~concerning the action to be taken specified in the alerts~~, it is appropriate to reinforce the functioning of the SIRENE Bureaux by specifying the requirements concerning the available resources, user training and the response time to the inquiries received from other SIRENE Bureaux.	
18		***(9a) In order to be able to fully exploit the functionalities of SIS, Member States should ensure that end-users and the staff of the SIRENE Bureaux regularly receive training, including on data security and protection. National standards for training end-users on data quality principles and***		*To be adapted in accordance with Art. 14*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		practice should be established in cooperation with the national SIRENE Bureau. Member States should call upon the staff of the SIRENE Bureaux to help train all authorities entering alerts, with a focus on data quality and maximising the use of SIS. The delivery of training should be in compliance with the Sirene Trainers' Manual. To the extent possible, SIRENE Bureaux should also provide for staff exchanges with other SIRENE Bureaux at least once a year. Member States are encouraged to take appropriate measures to avoid the loss of skills and experience through staff turnover.		
19				**New recital (9b) -Text from point 1.17.3 SIRENE Manual** (2018-03-26) (9b) Member States should ensure that the staff of the SIRENE bureau have the necessary linguistic skills and knowledge in relevant legislation and rules of procedure to perform their tasks.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
20	(10) The operational management of the central components of SIS are exercised by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice[10] (the Agency). In order to enable the Agency to dedicate the necessary financial and personal resources covering all aspects of the operational management of Central SIS, this Regulation should set out its tasks in detail, in particular with regard to the technical aspects of the exchange of supplementary information.		(10) The operational management of the central components of SIS are exercised by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice[9] (the Agency). In order to enable the Agency to dedicate the necessary financial and personal resources covering all aspects of the operational management of Central SIS **and the communication infrastructure**, this Regulation should set out its tasks in detail, in particular with regard to the technical aspects of the exchange of supplementary information.	*To adapted in accordance with Art. 15.*
21	(11) Without prejudice to the responsibility of Member States for the accuracy of data entered into SIS, the Agency should become responsible for reinforcing data quality by introducing a central data quality monitoring tool, and for providing reports at regular intervals to Member States.	(11) Without prejudice to the responsibility of Member States for the accuracy of data entered into SIS, the Agency should become responsible for reinforcing data quality by introducing a central data quality monitoring tool, and for providing reports at regular intervals to the Member States. ***To further increase the quality of data in SIS, the Agency should***	(11) Without prejudice to the **primary** responsibility of Member States for the accuracy of data entered into SIS, **and the role of the SIRENE Bureaux as quality coordinators,** the Agency should become responsible for reinforcing data quality by introducing a central data quality monitoring tool, and for providing reports at	

[10] Established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		also offer training on the use of SIS to national training bodies and, insofar as possible, to SIRENE staff and to end-users. Such training should focus in particular on measures to improve the quality of SIS data.	regular intervals to **the Commission and the** Member States.	
22	(12) In order to allow better monitoring of the use of SIS to analyse trends concerning criminal offences, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States, the Commission, Europol and the European Border and Cost Guard Agency without jeopardising data integrity. Therefore, a central statistical repository should be established. Any statistic produced should not contain personal data.	(12) In order to allow better monitoring of the use of SIS to analyse trends concerning migratory pressure and border management, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States, ***the European Parliament, the Council,*** the Commission, Europol and the European Border and Cost Guard Agency without jeopardising data integrity. Therefore, a central statistical repository should be established. Any statistic ***retained in the repository or*** produced ***by the repository*** should not contain personal data ***as defined in Regulation (EC) No 45/2001 of the European Parliament and of the Council[11].***	(12) In order to allow better monitoring of the use of SIS to analyse trends concerning criminal offences, the Agency should be able to develop a state-of-the-art capability for statistical reporting to the Member States, the Commission, Europol and the European Border and Cost Guard Agency without jeopardising data integrity. Therefore, a central statistical repository should be established. Any statistic produced should not contain personal data. **Member States should communicate statistics concerning the right of access, rectification of inaccurate data and erasure of unlawfully stored data to the cooperation mechanism.**	*To be adapted in accordance with Art. 49*

[11] ***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).***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
23	(13) SIS should contain further data categories to allow end-users to take informed decisions based upon an alert without losing time. Therefore, in order to facilitate the identification of persons and to detect multiple identities, data categories relating to persons should include a reference to the personal identification document or number and a copy of such document where available.	(13) SIS should contain further data categories to allow end-users to take informed decisions based upon an alert without losing time. Therefore, in order to facilitate identification **(...)** and **(...)** detect multiple identities, **the alert** should include a reference to the personal identification document or number and a ***colour*** copy of such document, where available.	(13) SIS should contain further data categories to allow end-users to take informed decisions based upon an alert without losing time. Therefore, in order to facilitate the identification of persons and to detect multiple identities, data categories relating to persons should include a reference to the personal identification document or number and a copy of such document where available.	*Linked with Art. 20*
24			**(13A) Where available, all the relevant data, in particular the forename, should be inserted when creating an alert, in order to minimize the risk of false hits and unnecessary operational activities.**	
25	(14) SIS should not store any data used for search with the exception of keeping logs to verify if the search is lawful, for monitoring the lawfulness of data processing, for self-monitoring and for ensuring the proper functioning of N.SIS, as well as for data integrity and security.		(14) SIS should not store any data used for search with the exception of keeping logs to verify if the search is lawful, for monitoring the lawfulness of data processing, for self-monitoring and for ensuring the proper functioning of N.SIS, as well as for data integrity and security.	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
26	(15) SIS should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. In the same perspective, SIS should also allow for the processing of data concerning individuals whose identity has been misused (in order to avoid inconveniences caused by their misidentification), subject to suitable safeguards; in particular with the consent of the individual concerned and a strict limitation of the purposes for which such data can be lawfully processed.	(15) SIS should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. ***Any entry and use of photographs, facial images, dactyloscopic data or DNA may not exceed what is necessary for the objectives pursued, must be authorised by Union law, take place in respect of fundamental rights, including the best interests of the child, and be in accordance with relevant provisions on data protection laid down in the SIS legal instruments, Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council[12].*** In the same perspective, SIS should also allow for the processing of data concerning individuals whose identity has been misused (in order to avoid inconveniences caused by their misidentification), subject to suitable safeguards; in particular with the consent of the individual concerned and a strict limitation of the purposes for which such	(15) SIS should permit the processing of biometric data in order to assist in the reliable identification of the individuals concerned. In the same perspective, SIS should also allow for the processing of data concerning individuals whose identity has been misused (in order to avoid inconveniences caused by their misidentification), subject to suitable safeguards; in particular with the consent of the individual concerned and a strict limitation of the purposes for which such data can be lawfully processed.	

[12] ***Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 20017 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of 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).***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		personal data can be lawfully processed.		
27	(16) Member States should make the necessary technical arrangement so that each time the end-users are entitled to carry out a search in a national police or immigration database they also search SIS in parallel in accordance with Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council[13]. This should ensure that SIS functions as the main compensatory measure in the area without internal border controls and better address the cross-border dimension of criminality and the mobility of criminals.	(16) Member States should make the necessary technical arrangement so that each time the end-users are entitled to carry out a search in a national police or immigration database they also search SIS in parallel in ***full respect of*** Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council ***and Article 5 of Regulation (EU) 2016/679***. This should ensure that SIS functions as the main compensatory measure in the area without internal border controls and better address the cross-border dimension of criminality and the mobility of criminals.	(16) Member States should make the necessary technical arrangement so that each time the end-users are entitled to carry out a search in a national police or immigration database they also search SIS in parallel in accordance with Article 4 of Directive (EU) 2016/680 of the European Parliament and of the Council[10]. This should ensure that SIS functions as the main compensatory measure in the area without internal border controls and better address the cross-border dimension of criminality and the mobility of criminals.	
28	(17) This Regulation should set out the conditions for use of dactylographic data and facial images for identification purposes. The use of facial images for identification purposes in SIS should also help to ensure	(17) This Regulation should set out the conditions for use of ***dactyloscopic*** data***, photographs*** and facial images for identification purposes. The use of ***dactyloscopic data and*** facial images for identification purposes in SIS should also help ensure consistency	(17) This Regulation should set out the conditions for use of ~~dactylographic~~**dactyloscopic** data and facial images for identification purposes. The use of facial images for identification purposes in SIS should **in particular**~~also~~ help to	

[13] 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 purposes of 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 (OJ L 119, 4.5.2016, p. 89).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	consistency in border control procedures where the identification and the verification of identity are required by the use of fingerprints and facial images. Searching with dactylographic data should be mandatory if there is any doubt concerning the identity of a person. Facial images for identification purposes should only be used in the context of regular border controls in self-service kiosks and electronic gates.	in border control procedures where identification and the verification of identity are required by the use of fingerprints and facial images. Searching with ***dactyloscopic*** data should be mandatory if ***the identity of the person cannot be ascertained by any other means***. ***To verify whether the person already appears in SIS under another identity or alert, it should be possible to carry out a fingerprint search before a new alert is entered.*** Facial images for identification purposes should only be used in the context of regular border controls in self-service kiosks and electronic gates.	ensure consistency in border control procedures where the identification and the verification of identity are required by the use of **dactyloscopic**~~fingerprints~~ and facial images. Searching with ~~dactylographic~~**dactyloscopic** data should be mandatory if there is any doubt concerning the identity of a person. ~~Facial images for identification purposes should only be used in the context of regular border controls in self-service kiosks and electronic gates.~~	
29	(18) The introduction of an automated fingerprint identification service within SIS complements the existing Prüm mechanism on mutual cross-border online access to designated national DNA databases and automated	(18) The introduction of an automated fingerprint identification service within SIS complements the existing Prüm mechanism on mutual cross-border online access to designated national DNA databases and automated fingerprint identification systems[15]. The Prüm mechanism enables	(18) The introduction of an automated fingerprint identification service within SIS complements the existing Prüm mechanism on mutual cross-border online access to designated national DNA databases and automated fingerprint identification systems[11]. The Prüm mechanism enables	

[15] 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); and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	fingerprint identification systems[14]. The Prüm mechanism enables interconnectivity of national fingerprint identification systems whereby a Member State can launch a request to ascertain if the perpetrator of a crime whose fingerprints have been found, is known in any other Member State. The Prüm mechanism verifies if the owner of the fingerprints are known in one point in time therefore if the perpetrator becomes known in any of the Member States later on he or she will not necessarily be captured. The SIS fingerprint search allows an active search of the perpetrator. Therefore, it should be possible to upload the fingerprints of an unknown perpetrator into SIS, provided that the owner of the fingerprints can be identified to a high degree of probability as the perpetrator of a serious crime or act of terrorism. This is in particular the case if fingerprints are found on the weapon or on any object used for the offence. The mere presence	interconnectivity of national fingerprint identification systems whereby a Member State can launch a request to ascertain if the perpetrator of a crime whose fingerprints have been found, is known in any other Member State. The Prüm mechanism verifies if the owner of the fingerprints are known in one point in time therefore if the perpetrator becomes known in any of the Member States later on he or she will not necessarily be captured. The SIS ***dactyloscopic data*** search allows an active search of the perpetrator. Therefore, it should be possible to upload the ***dactyloscopic data*** of an unknown perpetrator into SIS, provided that the owner of the ***dactyloscopic data*** can be identified to a ***very*** high degree of probability as the perpetrator of a serious crime or act of terrorism. This is in particular the case if ***dactyloscopic data*** are found on the weapon or on any object used for the offence. The mere presence of the ***dactyloscopic***	interconnectivity of national fingerprint identification systems whereby a Member State can launch a request to ascertain if the perpetrator of a crime whose fingerprints have been found, is known in any other Member State. The Prüm mechanism verifies if the owner of the fingerprints are known in one point in time**.** **T**therefore if the perpetrator becomes known in any of the Member States later on he or she will not necessarily be captured. The SIS fingerprint search allows an active search of the perpetrator. Therefore, it should be possible to upload the fingerprints of an unknown perpetrator into SIS, provided that the owner of the fingerprints can be identified to a high degree of probability as the perpetrator of a serious crime or act of terrorism. This is in particular the case if fingerprints are found on the weapon or on any object used for the offence. The mere presence of the fingerprints at the crime scene should not be considered as	

[14] 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); and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	of the fingerprints at the crime scene should not be considered as indicating a high degree of probability that the fingerprints are those of the perpetrator. A further precondition for the creation of such alert should be that the identity of the perpetrator cannot be established via any other national, European or international databases. Should such fingerprint search lead to a potential match the Member State should should carry out further checks with their fingerprints, possibly with the involvement of fingerprint experts to establish whether he or she is the owner of the prints stored in SIS, and should establish the identity of the person. The procedures should be subject of national law. An identification as the owner of an "unknown wanted person" in SIS may substantially contribute to the investigation and it may lead to an arrest provided that all conditions for an arrest are met.	***data*** at the crime scene should not be considered as indicating a ***very*** high degree of probability that the ***dactyloscopic data*** are those of the perpetrator. A further precondition for the creation of such alert should be that the identity of the perpetrator cannot be established via any other national, European or international databases. Should such fingerprint search lead to a potential match the Member State should carry out further checks with their fingerprints, possibly with the involvement of fingerprint experts to establish whether he or she is the owner of the prints stored in SIS, and should establish the identity of the person. The procedures should be subject of national law. An identification as the owner of an "unknown wanted person" in SIS may substantially contribute to the investigation and it may lead to an arrest provided that all conditions for an arrest are met.	indicating a high degree of probability that the fingerprints are those of the perpetrator. A further precondition for the creation of such alert should be that the identity of the perpetrator cannot be established via any other national, European or international databases. Should such fingerprint search lead to a potential match the Member State should ~~should~~ carry out further checks with their fingerprints, ~~possibly~~ **together** with the involvement of fingerprint experts to establish whether he or she is the owner of the prints stored in SIS, and should establish the identity of the person. The procedures should be subject of national law. An identification as the owner of an "unknown wanted person" in SIS may substantially contribute to the investigation and it may lead to an arrest provided that all conditions for an arrest are met.	
30	(19) Fingerprints found at a crime scene should be allowed to be checked against the fingerprints stored in SIS if it can be	(19) ***Complete or incomplete sets of fingerprints or palm prints*** found at a crime scene should be allowed to be checked against the dactylographic data stored in SIS if	(19) Fingerprints **or palmprints** found at a crime scene should be allowed to be checked against the **dactyloscopic data**~~fingerprints~~	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	established to a high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence. Serious crime should be the offences listed in Council Framework Decision 2002/584/JHA[16] and 'terrorist offence' should be offences under national law referred to in Council Framework Decision 2002/475/JHA[17].	it can be established to a ***very*** high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence ***provided that the competent authorities are unable to establish the identity of the person by using any other national, Union or international database***.	stored in SIS if it can be established to a high degree of probability that they belong to the perpetrator of the serious crime or terrorist offence. **Particular attention should be given to the establishement of quality standards appliable to the storage of biometric data, including latent dactyloscopic data.** Serious crime should be the offences listed in Council Framework Decision 2002/584/JHA[12] and 'terrorist offence' should be offences ~~under national law~~ **corresponding or equivalent to one of the offences** referred to in **Directive (EU) 2017/541**[18] ~~Council Framework Decision 2002/475/JHA[13]~~.	
31	(20) It should be possible to add a DNA profile in cases where dactylographic data are not available, and which should only be accessible to authorised users. DNA profiles should facilitate the	(20) It should be possible***, in a narrow band of clearly defined cases,*** to add a DNA profile in cases where ***dactyloscopic*** data are not available, and which should only be accessible to authorised	(20) It should be possible to add a DNA profile in cases where ~~dactylographic~~**dactyloscopic** data**, photographs or facial images** are not available, and which should only be accessible to authorised	

[16] Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (0J L 190, 18.07.2002, p. 1).

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

[18] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31/03/2017, p. 6.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	identification of missing persons in need of protection and particularly missing children, including by allowing the use of DNA profiles of parents or siblings to enable identification. DNA data should not contain reference to racial origin.	users. DNA profiles should facilitate the identification of missing persons in need of protection and particularly missing children, including by allowing the use of DNA profiles of parents or siblings to enable identification. DNA data should not contain ***references*** to racial origin ***or information about health or reveal any other sensitive data.***	users. DNA profiles should facilitate the identification of missing persons in need of protection and particularly missing children, including by allowing the use of DNA profiles of **ascendants, descendants** ~~parents~~ or siblings to enable identification. DNA data should not contain reference to racial origin.	
32			**(20A) It should be possible in all cases to identify a person by using dactyloscopic data. Wherever the identity of the person cannot be ascertained by any other means, dactyloscopic data should be used to attempt to ascertain the identity.**	
33			**(20B) DNA profiles should only be retrieved from SIS in case that an identification is necessary and proportionate for the purposes of Article 32(2)(a) and (c). DNA profiles should not be retrieved and processed for any other purpose than those for which they were entered in accordance with Article 32(2)(a) and (c). Applying the data**	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			protection and security rules laid down in this Regulation additional safeguards, if necessary, should be put in place when using DNA profiles in order to prevent any risks for false matches, hacking and unauthorised sharing with third parties.	
34	(21) SIS should contain alerts on persons wanted for arrest for surrender purposes and wanted for arrest for extradition purposes. In addition to alerts, it is appropriate to provide for the exchange of supplementary information which is necessary for the surrender and extradition procedures. In particular, data referred to in Article 8 of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States[19] should be processed in SIS. Due to operational reasons, it is appropriate for the issuing Member State to make an existing alert for		(21) SIS should contain alerts on persons wanted for arrest for surrender purposes and wanted for arrest for extradition purposes. In addition to alerts, it is appropriate to provide for the exchange of supplementary information **via the SIRENE Bureaux** which is necessary for the surrender and extradition procedures. In particular, data referred to in Article 8 of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member States[15] should be processed in SIS. Due to operational reasons, it is appropriate for the issuing Member	

[19] Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (0J L 190, 18.07.2002, p. 1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	arrest temporary unavailable upon the authorisation of the judicial authorities when a person subject of a European Arrest Warrant is intensively and actively searched and end-users not involved in the concrete search operation may jeopardise the successful outcome. The temporary unavailability of such alerts should not exceed 48 hours.		State to make an existing alert for arrest temporar**ly** unavailable upon the authorisation of the judicial authorities when a person subject of a European Arrest Warrant is intensively and actively searched and end-users not involved in the concrete search operation may jeopardise the successful outcome. The temporary unavailability of such alerts should **in principle** not exceed 48 hours.	
35	(22) It should be possible to add to SIS a translation of the additional data entered for the purpose of surrender under the European Arrest Warrant and for the purpose of extradition.		(22) It should be possible to add to SIS a translation of the additional data entered for the purpose of surrender under the European Arrest Warrant and for the purpose of extradition.	
36	(23) SIS should contain alerts on missing persons to ensure their protection or to prevent threats to public security. Issuing an alert in SIS for children at risk of abduction (*i.e.* in order to prevent a future harm that has not yet taken place as in the case of children who are at risk of parental abduction) should be limited, therefore it is appropriate to provide for strict and appropriate safeguards. In cases of	(23) SIS should contain alerts on missing persons to ensure their protection or to prevent threats to public security. Issuing an alert in SIS for children at risk of abduction (*i.e.* in order to prevent a future harm that has not yet taken place as in the case of children who are at risk of abduction ***or of being removed from the Member State for the purpose of torture, sexual or gender-based violence or of being victims of activities listed in***	(23) SIS should contain alerts on missing **or vulnerable** persons to ensure their protection or to prevent threats to public security. Issuing an alert in SIS for children at risk of abduction (*i.e.* in order to prevent a future harm that has not yet taken place as in the case of children who are at risk of parental abduction) should be limited, therefore it is appropriate to provide for ~~strict and~~ appropriate	(23) SIS should contain alerts on missing persons or on persons who need to be prevented from travelling to ensure their protection or to prevent threats to public security or public order. ~~Issuing an alert in SIS for children at risk of abduction, where there is a concrete and apparent risk of parental child abduction, should be limited, therefore it is appropriate to provide for strict and appropriate~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	children, these alerts and the corresponding procedures should serve the best interests of the child having regard to Article 24 of the Charter of Fundamental Rights of the European Union and the United Nations Convention on the Rights of the Child of 20 November 1989.	***Articles 6 to 10 of Directive (EU) 2017/541 of the European Parliament and of the Council***[20]) should be limited***. Therefore*** it is appropriate to provide for strict and appropriate safeguards, ***including the entering of such an alert only following a decision by a judicial authority***. In cases of children, these alerts and the corresponding procedures should serve the best interests of the child ***in accordance with*** Article 24 of the Charter of Fundamental Rights of the European Union ***and Article 3 of*** the United Nations Convention on the Rights of the Child of 20 November 1989. ***Law enforcement authorities' decisions on the action to be taken following an alert on a child should be taken in cooperation with child protection authorities. The national hotline for missing children should be informed.***	safeguards. In cases of children, these alerts and the corresponding procedures should serve the best interests of the child having regard to Article 24 of the Charter of Fundamental Rights of the European Union and the United Nations Convention on the Rights of the Child of 20 November 1989.	~~safeguards.~~ In cases of children, these alerts and the corresponding procedures should serve the best interests of the child ***in accordance with*** Article 24 of the Charter of Fundamental Rights of the European Union ***and Article 3 of*** the United Nations Convention on the Rights of the Child of 20 November 1989. ***Actions and decisions by the competent authorities, including judicial authorities, following an alert on a child should be taken in cooperation with child protection authorities. The national hotline for missing children should be informed*** where appropriate**.**
37		***(23a) Regarding alerts for children at risk, in assessing whether a concrete and apparent risk exists that a child may be***	**(23A) Alerts on children at risk of abduction should be entered to SIS at the request of competent authorities, including judicial**	**(23A) Alerts on missing persons who need to be placed under protection should be entered at the request of the competent**

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

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		unlawfully and imminently removed from the Member State, the competent judicial authority should take into account the child's personal circumstances and the environment to which her or she is exposed.	**authorities having jurisdictions in matters of parental responsibility in accordance with national law.**	**~~judicial~~ authority. All children who have gone missing from Member States' reception facilities should be entered in SIS as missing persons.**
38			**(23B) Alerts on vulnerable persons who need to be prevented from travelling for their own protection should be entered for example with respect to whom it is believed that the travel would create a risk of forced mariage, female genital mutilation, traficking of human beings or in the case of children, of joining armed conflicts, organised criminal groups or terrorist groups.**	**(23B) Alerts on children at risk of parental child abduction should be entered** in **SIS at the request of competent authorities, including judicial authorities having jurisdiction in matters of parental responsibility in accordance with national law.** Issuing an alert in SIS for children at risk of **parental child** abduction, where this risk is concrete and apparent, should be limited, therefore it is appropriate to provide for strict and appropriate safeguards. ***In assessing whether a concrete and apparent risk exists that a child may be unlawfully and imminently removed from a Member State, the competent ~~judicial~~ authority should take into account the child's personal circumstances and the environment to which ~~her or she~~*** *the child* ***is exposed.***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
39				*Informal outcome of techical discussion* **(23C) This Regulation should establish a new category of alerts for certain categories of vulnerable persons who need to be prevented from travelling. Persons who, due to their age, disabilities, or their family circumstances require protection should be considered vulnerable.**
40				**(23D) Alerts on** *children* **who need to be prevented from travelling for their own protection should be entered** in SIS ***if there is a concrete and apparent risk of them being*** **removed from or leaving the territory of a Member** ***State. Such alerts should be entered if the travel would put them at risk of becoming victims*** of **trafficking of human beings** or of **forced marriage, female genital mutilation or other forms of gender-based violence, or** at risk of becoming victims or being involved in the offences listed in Articles 6 to 10 of Directive (EU) 2017/541, or, at risk of being

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				conscripted or enlisted into armed groups or of being made to participate actively in hostilities.
41				(23**E**) **Alerts on vulnerable adults who need to be prevented from travelling for their own protection should be entered if travel would put them at risk of becoming victims of trafficking of human beings or gender-based violence.**
42				**(23F) In order to guarantee strict and appropriate safeguards the alerts on children or other vulnerable persons who need to be prevented from travelling should, where required under national law, be entered into SIS following a decision by a judicial authority or a decision by a competent authority confirmed by a judicial authority.**
43	(24) A new action should be included for cases of suspected terrorism and serious crime, allowing for a person who is suspected to have committed a serious crime or where there is a	(24) ***Without prejudice to the rights of suspects and accused persons, in particular, to their right to have access to a lawyer in accordance with Directive 2013/48/EU of the European***	(24) A new action should be included for cases of suspected terrorism and serious crime, allowing for a person who is suspected to have committed a serious crime or where there is a	(24) A new action should be introduced for cases ***where, based on a clear indication, a person is suspected of intending to commit or of committing*** **any of the offences referred to in Article 2(1)**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	reason to believe that he or she will commit a serious crime, to be stopped and questioned in order to supply the most detailed information to the issuing Member State. This new action should not amount either to searching the person or to his or her arrest. It should supply, however, sufficient information to decide about further actions. Serious crime should be the offences listed in Council Framework Decision 2002/584/JHA.	***Parliament and of the Council[21], a*** new action should be included for cases ***where, based on a clear indication, a person is suspected of intending to commit or of committing*** a serious crime ***or where the relevant information is necessary for the execution of a criminal sentence of a person convicted of a serious crime*** or where there is a reason to believe that he or she will commit a serious crime, ***to allow that person*** to be stopped and questioned in order to supply the most detailed information to the issuing Member State ***(inquiry check)***. This new action should not amount either to searching the person or to his or her arrest. It should supply, however, sufficient information to decide about further actions.	reason to believe that he or she will commit a serious crime, to be ~~stopped and~~ **interviewed.**~~questioned~~ **subject to national law** in order to supply the most detailed information to the issuing Member State. This new action **to be carried out during the police or border check** should not amount either to searching the person or to his or her arrest **and the procedural rights of the person should be preserved**. **It is also without prejudice to existing mutual legal assistance mechanisms.** It should supply, however, sufficient information to decide about further actions **between the alert issuing and executing authorities as much as possible in real time**. Serious crime should be the offences listed in Council Framework Decision 2002/584/JHA.	**and (2) of Framework Decision 2002/584/JHA.** ***A new action should also be included where the relevant information is necessary for the execution of a custodial sentence or detention order against a person convicted of*** **any of the offences referred to in Article 2(1) and (2) of Framework Decision 2002/584/JHA,** or where there is a reason to believe that he or she will commit **any of those offences**, ***to allow that person*** to be stopped and ~~questioned~~ ***interviewed*** in order to supply the most detailed information to the issuing Member State . ***This action should be also without prejudice to existing mutual legal assistance mechanisms. It*** should supply sufficient information to decide about further actions. ***This new action to be carried out during a police or border check*** should not amount ~~either~~ to searching the person nor to his or her arrest ***and the procedural rights of suspects***

[21] Directive 2013/48/EU of the European Parliament and of the Council of of 22 October 2013 on the right of access to a lawyer in criminal proceeding sand in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294. 6,11,2013, p. 1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				and accused persons under Union and national law should be preserved, including their right to have access to a lawyer in accordance with Directive 2013/48/EU of the European Parliament and of the Council.
44			**(24A) In case of alerts on objects for seizure or use as evidence in criminal proceedings, the objects should in principle be seized. However, national law determines if and in accordance with which conditions an object is seized, particularly if it is in the possession of its rightful owner.**	
45	(25) SIS should contain new categories of objects of high value, such as electronic and technical equipment which can be identified and searched with a unique number.		(25) SIS should contain new categories of objects of high value, such as **information technology items**~~electronic and technical equipment~~ which can be identified and searched with a unique number.	
46			**(25A) As regards documents to be inserted for seizure or use as evidence in criminal proceedings, the term "false" should be construed as encompassing both**	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			falsified and counterfeit documents.	
47	(26) It should be possible for a Member State to add an indication, called a flag, to an alert, to the effect that the action to be taken on the basis of the alert will not be taken on its territory. When alerts are issued for arrest for surrender purposes, nothing in this Decision should be construed so as to derogate from or prevent the application of the provisions contained in the Framework Decision 2002/584/JHA. The decision to add a flag to an alert should be based only on the grounds for refusal contained in that Framework Decision.	(26) It should be possible for a Member State to add an indication, called a flag, to an alert, to the effect that the action to be taken on the basis of the alert will not be taken on its territory ***including in cases of alerts for the purposes of inquiry checks***. When alerts are issued for arrest for surrender purposes, nothing in this ***Regulation*** should be construed so as to derogate from or prevent the application of the provisions contained in the Framework Decision 2002/584/JHA. The decision to add a flag to an alert should be based only on the grounds for refusal contained in that Framework Decision.	(26) It should be possible for a Member State to add an indication, called a flag, to an alert, to the effect that the action to be taken on the basis of the alert will not be taken on its territory. When alerts are issued for arrest for surrender purposes, nothing in this **Regulation** ~~Decision~~ should be construed so as to derogate from or prevent the application of the provisions contained in the Framework Decision 2002/584/JHA. The decision to add a flag to an alert **with a view to non-executing a European Arrest Warrant** should be based only on the grounds for refusal contained in that Framework Decision.	
48	(27) When a flag has been added and the whereabouts of the person wanted for arrest for surrender becomes known, the whereabouts should always be communicated to the issuing judicial authority, which may decide to transmit a European Arrest Warrant to the competent judicial authority in		(27) When a flag has been added and the whereabouts of the person wanted for arrest for surrender becomes known, the whereabouts should always be communicated to the issuing judicial authority, which may decide to transmit a European Arrest Warrant to the competent judicial authority in	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	accordance with the provisions of the Framework Decision 2002/584/JHA.		accordance with the provisions of the Framework Decision 2002/584/JHA.	
49	(28) It should be possible for Member States to establish links between alerts in SIS. The establishment by a Member State of links between two or more alerts should have no impact on the action to be taken, their retention period or the access rights to the alerts.		(28) It should be possible for Member States to establish links between alerts in SIS. The establishment by a Member State of links between two or more alerts should have no impact on the action to be taken, their retention period or the access rights to the alerts.	
50	(29) Alerts should not be kept in SIS longer than the time required to fulfil the purposes for which they were issued. In order to reduce the administrative burden on the different authorities involved in processing data on individuals for different purposes, it is appropriate to align the retention period of alerts on persons with the retention periods envisaged for return and illegal stay purposes. Moreover, Member States regularly extend the expiry date of alerts on persons if the required action could not be taken within the original time period. Therefore, the retention period for	(29) Alerts should not be kept in SIS longer than the time required to fulfil the ***specific*** purposes for which they were issued. Therefore, the ***review*** period for alerts on persons should be a maximum of ***three*** years. As a general principle, alerts on persons should be deleted from SIS after a period of ***three*** years, except for alerts issued for the purposes of discreet, specific and inquiry checks. These should be deleted after one year. Alerts on objects entered for discreet checks, inquiry checks or specific checks should be automatically deleted from the SIS after a period of one year, as they are always related to persons. Alerts on objects for	(29) Alerts should not be kept in SIS longer than the time required to fulfil the purposes for which they were issued. In order to reduce the administrative burden on the different authorities involved in processing data on individuals for different purposes, it is appropriate to align the retention period of alerts on persons with the retention periods envisaged for return and illegal stay purposes. Moreover, Member States regularly extend the expiry date of alerts on persons if the required action could not be taken within the original time period. Therefore, the retention period for	*To be aligned with Art. 51.*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	alerts on persons should be a maximum of five years. As a general principle, alerts on persons should be automatically deleted from SIS after a period of five years, except for alerts issued for the purposes of discreet, specific and inquiry checks. These should be deleted after one year. Alerts on objects entered for discreet checks, inquiry checks or specific checks should be automatically deleted from the SIS after a period of one year, as they are always related to persons. Alerts on objects for seizure or use as evidence in criminal proceedings should be automatically deleted from SIS after a period of five years, as after such a period the likelihood of finding them is very low and their economic value is significantly diminished. Alerts on issued and blank identification documents should be kept for 10 years, as the validity period of documents is 10 years at the time of issuance. Decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons within the	seizure or use as evidence in criminal proceedings should be automatically deleted from SIS after a period of five years, as after such a period the likelihood of finding them is very low and their economic value is significantly diminished. Alerts on issued and blank identification documents should be kept for 10 years, as the validity period of documents is 10 years at the time of issuance. Decisions to keep alerts on persons should be based on a comprehensive individual assessment. Member States should review alerts on persons within the defined period and keep statistics about the number of alerts on persons for which the retention period has been extended.	alerts on persons should be a maximum of five years. As a general principle, alerts on persons should be automatically deleted from SIS after a period of five years, except for alerts issued for the purposes of discreet, specific and inquiry checks. These should be deleted after one year. Alerts on objects ~~entered for discreet checks, inquiry checks or specific checks should be automatically deleted from the SIS after a period of one year, as they are always related to persons. Alerts on objects for seizure or use as evidence in criminal proceedings~~ should be automatically deleted from SIS after a period of **ten**~~five~~ years, as after such a period the likelihood of finding them is very low and their economic value is significantly diminished. Alerts on **objects, where linked to alerts on persons** ~~issued and blank identification documents~~ should **not** be kept **longer than the linked alert on the person and in any case not exceeding five**~~for 10~~ years~~, as the validity period of documents is 10 years at the time of issuance~~. Decisions to keep alerts on persons	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	defined period and keep statistics about the number of alerts on persons for which the retention period has been extended.		should be based on a comprehensive individual assessment. Member States should review alerts on persons **and objects** within ~~the~~ **regular** ~~defined~~ period**s** and keep statistics about the number of alerts ~~on persons~~ for which the retention period has been extended.	
51	(30) Entering and extending the expiry date of a SIS alert should be subject to the necessary proportionality requirement, examining whether a concrete case is adequate, relevant and important enough to insert an alert in SIS. Offences pursuant to Articles 1, 2, 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism[22] constitute a very serious threat to public security and integrity of life of individuals and to society, and these offences are extremely difficult to prevent, detect and investigate in an area without internal border controls where potential offenders circulate freely.	(30) Entering and extending the expiry date of a SIS alert should be subject to the necessary proportionality requirement, examining whether a concrete case is adequate, relevant and important enough to insert an alert in SIS. Offences pursuant to ***Directive (EU) 2017/541*** constitute a very serious threat to public security and integrity of life of individuals and to society, and these offences are extremely difficult to prevent, detect and investigate in an area without internal border controls where potential offenders circulate freely. Where a person or object is sought in relation to these offences, it is always necessary to create the	(30) Entering and extending the expiry date of a SIS alert should be subject to the necessary proportionality requirement, examining whether a concrete case is adequate, relevant and important enough to insert an alert in SIS. Offences pursuant to Articles **3 to 14 of Directive (EU) 2017/541**[23] ~~1, 2, 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism~~[16] constitute a very serious threat to public security and integrity of life of individuals and to society, and these offences are extremely difficult to prevent, detect and investigate in an area without internal border controls where	*Consistency with (24) in PolCoop to be checked.* *Linked to Art. 21.*

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

23 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31/03/2017, p. 6.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Where a person or object is sought in relation to these offences, it is always necessary to create the corresponding alert in SIS on persons sought for a criminal judicial procedure, on persons or objects subject to a discreet, inquiry and specific check as well as on objects for seizure, as no other means would be as effective in relation to that purpose.	corresponding alert in SIS on persons sought for a criminal judicial procedure, on persons or objects subject to a discreet, inquiry and specific check as well as on objects for seizure, as no other means would be as effective in relation to that purpose.	potential offenders circulate freely. Where a person or object is sought in relation to these offences, it is ~~always~~ necessary to create the corresponding alert in SIS on persons sought for a criminal judicial procedure, on persons or objects subject to a discreet, inquiry**,** and specific check as well as on objects for seizure, as no other means would be as effective in relation to that purpose. **Exceptionally, Member States may refrain from creating the alert when it is likely to obstruct official or legal inquiries, investigations or procedures related to public or national security.**	
52	(31) It is necessary to provide clarity concerning the deletion of alerts. An alert should be kept only for the time required to achieve the purpose for which it was entered. Considering the diverging practices of Member States concerning the definition of the point in time when an alert fulfils its purpose, it is appropriate to set out detailed criteria for each alert category to	(31) It is necessary to provide ***rules*** concerning the deletion of alerts. An alert should be kept only for the time required to achieve the purpose for which it was entered. Considering the diverging practices of Member States concerning the definition of the point in time when an alert fulfils its purpose, it is appropriate to set out detailed criteria for each alert category to determine when it	(31) It is necessary to provide clarity concerning the deletion of alerts. An alert should be kept only for the time required to achieve the purpose for which it was entered. Considering the diverging practices of Member States concerning the definition of the point in time when an alert fulfils its purpose, it is appropriate to set out detailed criteria for each alert category to	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	determine when it should be deleted from SIS.	should be deleted from SIS.	determine when it should be deleted from SIS.	
53	(32) The integrity of SIS data is of primary importance. Therefore, appropriate safeguards should be provided to process SIS data at central as well as at national level to ensure the end-to-end security of data. The authorities involved in data processing should be bound by the security requirements of this Regulation and be subject to a uniform incident reporting procedure.	(32) The integrity of SIS data is of primary importance. Therefore, appropriate safeguards should be provided to process SIS data at central as well as at national level to ensure the end-to-end security of data. The authorities involved in data processing should be bound by the security requirements of this Regulation***, be appropriately trained for that purpose,*** be subject to a uniform incident reporting procedure ***and be informed of any offences and criminal penalties in this respect***.	(32) The integrity of SIS data is of primary importance. Therefore, appropriate safeguards should be provided to process SIS data at central as well as at national level to ensure the end-to-end security of data. The authorities involved in data processing should be bound by the security requirements of this Regulation and be subject to a uniform incident reporting procedure.	*Linked to Article 57*.
54	(33) Data processed in SIS in application of this Regulation should not be transferred or made available to third countries or to international organisations. However, it is appropriate to strengthen cooperation between the European Union and Interpol by promoting an efficient exchange of passport data. Where personal data is transferred from SIS to Interpol, these personal data should be subject to an adequate level of protection, guaranteed by an	(33) Data processed in SIS ***and the related supplementary information exchanged*** pursuant to this Regulation should not be transferred or made available to third countries or to international organisations.	(33) Data processed in SIS in application of this Regulation should not be transferred or made available to third countries or to international organisations. ~~However, it is appropriate to strengthen cooperation between the European Union and Interpol by promoting an efficient exchange of passport data. Where personal data is transferred from SIS to Interpol, these personal data should be subject to an adequate level of protection, guaranteed by an~~	*Linked to Article 62*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	agreement, providing strict safeguards and conditions.		~~agreement, providing strict safeguards and conditions.~~	
55	(34) It is appropriate to grant access to SIS to authorities responsible for registering vehicles, boats and aircraft in order to allow them to verify whether the conveyance is already searched for in a Member States for seizure or for check. Direct access should be provided to authorities which are governmental services. This access should be limited to alerts concerning the respective conveyances and their registration document or number plate. Accordingly, the provisions of Regulation (EC) 1986/2006 of the European Parliament and of the Council[24] should be included into this Regulation and that Regulation should be repealed.	(34) It is appropriate to grant ***direct*** access to SIS to ***competent*** authorities responsible for registering vehicles, boats and aircraft in order to allow them to verify whether the conveyance is already searched for in a Member States for seizure or for check. This access should be limited to alerts concerning the respective conveyances and their registration document or number plate. Accordingly, the provisions of Regulation (EC) 1986/2006 of the European Parliament and of the Council[25] should be included into this Regulation and that Regulation should be repealed.	(34) It is appropriate to grant access to SIS to authorities responsible for registering vehicles, boats and aircraft in order to allow them to verify whether the conveyance is already searched for in a Member States for seizure or for check. ~~Direct access should be provided to authorities which are governmental services. This access should be limited to alerts concerning the respective conveyances and their registration document or number plate. Accordingly, the provisions of Regulation (EC) 1986/2006 of the European Parliament and of the Council[18] should be included into this Regulation and that Regulation should be repealed.~~[26]	
56			**(34A) It is appropriate to grant access to SIS to authorities responsible for registering**	

[24] Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).

[25] Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).

[26] Moved to recital (34B).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			firearms in order to allow them to verify whether the firearm is already searched for in Member States for seizure or for check or whether there is an alert concerning the requesting person.	
57			**(34B)[27]Direct access should be provided to competent authorities which are governmental services. This access should be limited to alerts concerning the respective conveyances and their registration document or number plate or firearms and requesting persons. Accordingly, the provisions of Regulation (EC) 1986/2006 of the European Parliament and of the Council[28] should be included into this Regulation and that Regulation should be repealed. Any hit in SIS must be reported by the above mentioned authorities to the police authorities for further procedures in line with the particular alert in SIS and for**	

[27] Partially moved from recital (34).

[28] Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			notifying the hit via the SIRENE Bureaux to the issuing Member State.	
58	(35) For processing of data by competent national authorities for the purposes of the prevention, investigation, detection of serious crime or terrorist offences, or prosecution of criminal offences and the execution of criminal penalties including the safeguarding against the prevention of threat to public security, national provisions transposing Directive (EU) 2016/680 should apply. The provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council[29] and Directive (EU) 2016/680 should be further specified in this Regulation where necessary.	(35) ***National provisions transposing Directive (EU) 2016/680 should apply to the*** processing of ***personal*** data by competent authorities ***of the Member States*** for the purposes of the prevention, ***detection***, investigation of serious crime or terrorist offences, or prosecution of criminal offences, the execution of criminal penalties ***and*** the safeguarding against ***threats*** to public security***. Only designated authorities which are responsible for the prevention, detection or investigation of terrorist offences or other serious criminal offences and which Member States can guarantee apply all provisions of this Regulation and those of Directive (EU) 2016/680 as transposed into national law in a manner subject to verification by the competent authorities, including the supervisory authority established in***	(35) For processing of data by competent national authorities for the purposes of the prevention, investigation, detection of serious crime or terrorist offences, or prosecution of criminal offences and the execution of criminal penalties including the safeguarding against the prevention of threat to public security, national provisions transposing Directive (EU) 2016/680 should apply. The provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council[22] and Directive (EU) 2016/680 should be further specified in this Regulation where necessary.	

[29] 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).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		accordance with Article 41(1) of Directive (EU) 2016/680 and whose application of this Regulation is subject to evaluation through the mechanism established by Council Regulation (EU) No 1053/2013 should be entitled to consult the data stored in SIS.		
59	(36) Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation by national authorities when Directive (EU) 2016/680 does not apply. Regulation (EC) No 45/2001 of the European Parliament and of the Council[30] should apply to the processing of personal data by the institutions and bodies of the Union when carrying out their responsibilities under this Regulation.	(36) 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 ***competent authorities*** of the ***Member States for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties or safeguarding against threats to public security***.	(36) Regulation (EU) 2016/679 should apply to the processing of personal data under this Regulation by national authorities when Directive (EU) 2016/680 does not apply. Regulation (EC) No 45/2001 of the European Parliament and of the Council[31] should apply to the processing of personal data by the institutions and bodies of the Union when carrying out their responsibilities under this Regulation.	*Linked to Article 64*.
60		***(36a) Regulation (EC) No 45/2001 should apply to the processing of personal data by the institutions and bodies of the***		

[30] 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).

[31] 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).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		Union when carrying out their responsibilities under this Regulation.		
61		***(36b) Regulation (EU) 2016/794 of the European Parliament and of the Council[32] should apply to the processing of personal data by Europol under this Regulation.***		
62		***(36c) The provisions of Directive (EU) 2016/680, Regulation (EU) 2016/679, Regulation (EU) 2016/794 and Regulation (EC) No 45/2001 should be further specified in this Regulation where necessary.***		
63	(37) The provisions of Directive (EU) 2016/680, Regulation (EU) 2016/679 and Regulation (EC) No 45/2001 should be further specified in this Regulation where necessary. With regard to processing of personal data by Europol, Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement		(37) The provisions of Directive (EU) 2016/680, Regulation (EU) 2016/679 and Regulation (EC) No 45/2001 should be further specified in this Regulation where necessary. With regard to processing of personal data by Europol, Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement cooperation (Europol Regulation)[25] applies. **With regard to**	

[32] ***Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 25.5.2016, p. 53).***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	cooperation (Europol Regulation)[33] applies.		**processing of personal data by Eurojust, Decision 2002/187 applies.**	
64	(38) The provisions of Decision 2002/187/JHA of 28 February 2002[34] setting up Eurojust with a view to reinforcing the fight against serious crime concerning data protection apply to the processing of SIS data by Eurojust, including the powers of the Joint Supervisory Body, set up under that Decision, to monitor the activities of Eurojust and liability for any unlawful processing of personal data by Eurojust. In cases when searches carried out by Eurojust in SIS reveal the existence of an alert issued by a Member State, Eurojust cannot take the required action. Therefore it should inform the Member State concerned allowing it to follow up the case.	(38) ***Council*** Decision 2002/187/JHA[35] setting up Eurojust with a view to reinforcing the fight against serious crime ***should*** apply to the processing of ***personal data in SIS*** by Eurojust, including the powers of the Joint Supervisory Body, set up under that Decision, to monitor the activities of Eurojust and liability for any unlawful processing of personal data by Eurojust. In cases when searches carried out by ***national members of*** Eurojust ***and their assistants*** in SIS reveal the existence of an alert issued by a Member State, Eurojust ***should not be able to*** take the required action. Therefore it should ***immediately*** inform the Member State concerned allowing it to follow up the case.	(38) The provisions of Decision 2002/187/JHA of 28 February 2002[26] setting up Eurojust with a view to reinforcing the fight against serious crime concerning data protection apply to the processing of SIS data by Eurojust, including the powers of the Joint Supervisory Body, set up under that Decision, to monitor the activities of Eurojust and liability for any unlawful processing of personal data by Eurojust. In cases when searches carried out by Eurojust in SIS reveal the existence of an alert issued by a Member State, Eurojust cannot take the required action. Therefore it should inform the Member State concerned allowing it to follow up the case.	

33 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 25.5.2016, p. 53).

34 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1).

35 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
65	(39) In so far 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.		(39) In so far 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.	
66	(40) Both the Member States and the Agency 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 from a common perspective.		(40) Both the Member States and the Agency 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 from a common perspective.	
67	(41) The national independent supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States in relation to this Regulation. The rights of data subjects for access, rectification and erasure of their personal data stored in SIS, and subsequent remedies before national courts as well as the mutual recognition of judgments should be set out. Therefore, it is appropriate to	(41) The national independent supervisory authorities ***established in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680 (supervisory authorities)*** should monitor the lawfulness of the processing of personal data by the Member States in relation to this Regulation ***including the exchange of supplementary information, and should be granted sufficient resources to carry out this task.*** The rights of	(41) The national independent supervisory authorities should monitor the lawfulness of the processing of personal data by the Member States in relation to this Regulation. The rights of data subjects for access, rectification and erasure of their personal data stored in SIS, and subsequent remedies before national courts as well as the mutual recognition of judgments should be set out. Therefore, it is appropriate to	*Linked to Art. 67*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	require annual statistics from Member States.	data subjects for access, rectification, ***restriction of processing*** and erasure of their personal data stored in SIS, and subsequent remedies before national courts as well as the mutual recognition of judgments should be set out. Therefore, it is appropriate to require annual statistics from Member States.	require annual statistics from Member States.	
68	(42) The supervisory authorities should ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit should either be carried out by the supervisory authorities, or the national supervisory authorities should directly order the audit from an independent data protection auditor. The independent auditor should remain under the control and responsibility of the national supervisory authority or authorities which therefore should order the audit itself and provide a clearly defined purpose, scope and methodology of the audit as well as guidance and		(42) The supervisory authorities should ensure that an audit of the data processing operations in **their**~~its~~ N.SIS is carried out in accordance with international auditing standards at least every four years. The audit should either be carried out by the supervisory authorities, or the national supervisory authorities should directly order the audit from an independent data protection auditor. The independent auditor should remain under the control and responsibility of the national supervisory authority or authorities which therefore should order the audit itself and provide a clearly defined purpose, scope and methodology of the audit as well as guidance and supervision	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	supervision concerning the audit and its final results.		concerning the audit and its final results.	
69		***(42a) The European Data Protection Supervisor should monitor the activities of the Union institutions and bodies in relation to the processing of personal data under this Regulation. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of SIS.***		*Linked to Art. 67*.
70	(43) Regulation (EU) 2016/794 (Europol Regulation) provides that Europol supports and strengthens actions carried out by the competent authorities of Member States and their cooperation in combating terrorism and serious crime and provides analysis and threat assessments. The extension of Europol's access rights to the SIS alerts on missing persons should further improve Europol's capacity to provide national law enforcement authorities with comprehensive operational and analytical products concerning trafficking in human beings and child sexual exploitation, including	(43) Regulation (EU) 2016/794 (Europol Regulation) provides that Europol supports and strengthens actions carried out by the competent authorities of Member States and their cooperation in combating terrorism and serious crime and provides analysis and threat assessments. The extension of Europol's access rights to the SIS alerts on missing persons should further improve Europol's capacity to provide national law enforcement authorities with comprehensive operational and analytical products concerning trafficking in human beings and child sexual exploitation, including	(43) Regulation (EU) 2016/794 (Europol Regulation) provides that Europol supports and strengthens actions carried out by the competent authorities of Member States and their cooperation in combating terrorism and serious crime and provides analysis and threat assessments. The extension of Europol's access rights to the SIS alerts on missing persons should further improve Europol's capacity to provide national law enforcement authorities with comprehensive operational and analytical products concerning trafficking in human beings and child sexual exploitation, including	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	online. This would contribute to better prevention of these criminal offences, the protection of potential victims and to the investigation of perpetrators. Europol's European Cybercrime Centre would also benefit from new Europol access to SIS alerts on missing persons, including in cases of travelling sex offenders and child sexual abuse online, where perpetrators often claim that they have access to children or can get access to children who might have been registered as missing. Furthermore, since Europol's European Migrant Smuggling Centre plays a major strategic role in countering the facilitation of irregular migration, it should obtain access to alerts on persons who are refused entry or stay within the territory of a Member State either on criminal grounds or because of non-compliance with visa and stay conditions.	online. This would contribute to better prevention of these criminal offences, the protection of potential victims and to the investigation of perpetrators. Europol's European Cybercrime Centre would also benefit from new Europol access to SIS alerts on missing persons, including in cases of travelling sex offenders and child sexual abuse online, where perpetrators often claim that they have access to children or can get access to children who might have been registered as missing.	online. This would contribute to better prevention of these criminal offences, the protection of potential victims and to the investigation of perpetrators. Europol's European Cybercrime Centre would also benefit from new Europol access to SIS alerts on missing persons, including in cases of travelling sex offenders and child sexual abuse online, where perpetrators often claim that they have access to children or can get access to children who might have been registered as missing. ~~Furthermore, since Europol's European Migrant Smuggling Centre plays a major strategic role in countering the facilitation of irregular migration, it should obtain access to alerts on persons who are refused entry or stay within the territory of a Member State either on criminal grounds or because of non-compliance with visa and stay conditions.~~	
71	(44) In order to bridge the gap in information sharing on terrorism, in particular on foreign terrorist fighters – where monitoring of their movement is crucial –	(44) In order to bridge the gap in information sharing on terrorism, in particular on foreign terrorist fighters – where monitoring of their movement is crucial – Member States should share	(44) In order to bridge the gap in information sharing on terrorism, in particular on foreign terrorist fighters – where monitoring of their movement is crucial –	*Linked to Art. 46*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Member States should share information on terrorism-related activity with Europol in parallel to introducing an alert in SIS, as well as hits and related information. This should allow Europol's European Counter Terrorism Centre to verify if there is any additional contextual information available in Europol's databases and to deliver high quality analysis contributing to disrupting terrorism networks and, where possible, preventing their attacks.	information on terrorism-related activity with Europol in parallel to introducing an alert in SIS, as well as hits**,** related information ***and information in case the action to be taken cannot be carried out***. ***Such sharing of information should take place in accordance with the applicable data protection provisions laid down in Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2016/794.***	Member States ~~should~~ **may** share information on terrorism-related activity with Europol **when** ~~in parallel to~~ introducing an alert in SIS, as well as hits and related information. **This information sharing should be carried out by the exchange of supplementary information with Europol on corresponding alerts. For this purpose Europol should set up a connection with the SIRENE communication infrastructure.** This should allow Europol's European Counter Terrorism Centre to verify if there is any additional contextual information available in Europol's databases and to deliver high quality analysis contributing to disrupting terrorism networks and, where possible, preventing their attacks.	
72	(45) It is also necessary to set out clear rules for Europol on the processing and downloading of SIS data to allow the most comprehensive use of SIS provided that data protection standards are respected as provided in this Regulation and Regulation (EU) 2016/794. In cases where searches	(45) It is also necessary to set out clear rules for Europol on the processing and downloading of SIS data to allow the most comprehensive use of SIS provided that data protection standards are respected as provided in this Regulation and Regulation (EU) 2016/794. In cases where searches carried out by Europol in SIS	(45) It is also necessary to set out clear rules for Europol on the processing and downloading of SIS data to allow the most comprehensive use of SIS provided that data protection standards are respected as provided in this Regulation and Regulation (EU) 2016/794. In cases where searches	*Linked to Art. 46*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	carried out by Europol in SIS reveal the existence of an alert issued by a Member State, Europol cannot take the required action. Therefore it should inform the Member State concerned allowing it to follow up the case.	reveal the existence of an alert issued by a Member State, Europol cannot take the required action. Therefore it should ***immediately*** inform the Member State concerned allowing it to follow up the case.	carried out by Europol in SIS reveal the existence of an alert issued by a Member State, Europol cannot take the required action. Therefore it should inform the Member State concerned **via the exchange of supplementary information with the respective SIRENE Bureau** allowing it to follow up the case.	
73	(46) Regulation (EU) 2016/1624 of the European Parliament and of the Council[36] provides for the purpose of this Regulation, that the host Member State is to authorise the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks, deployed by the European Border and Coast Guard Agency, to consult European databases, where this consultation is necessary for fulfilling operational aims specified in the operational plan on border checks,	(46) Regulation (EU) 2016/1624 of the European Parliament and of the Council[37] provides for the purpose of this Regulation, that the host Member State is to authorise the members ***of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624*** deployed by the European Border and Coast Guard Agency, to consult European databases, where this consultation is necessary for fulfilling operational aims specified in the operational plan on border checks, border surveillance and return. Other relevant Union	(46) Regulation (EU) 2016/1624 of the European Parliament and of the Council[27] provides for the purpose of this Regulation, that the host Member State is to authorise the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks, deployed by the European Border and Coast Guard Agency, to consult European databases, where this consultation is necessary for fulfilling operational aims specified in the operational plan on border checks,	*Linked to Art. 48*.

[36] 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 of 16.9.2016, p. 1).

[37] 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 of 16.9.2016, p. 1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	border surveillance and return. Other relevant Union agencies, in particular the European Asylum Support Office and Europol, may also deploy experts as part of migration management support teams, who are not members of the staff of those Union agencies. The objective of the deployment of the European Border and Coast Guard teams, teams of staff involved in return-related tasks and the migration management support team is to provide for technical and operational reinforcement to the requesting Member States, especially to those facing disproportionate migratory challenges. Fulfilling the tasks assigned to the European Border and Coast Guard teams, teams of staff involved in return-related tasks and the migration management support team necessitates access to SIS via a technical interface of the European Border and Coast Guard Agency connecting to Central SIS. In cases where searches carried out by the team or the teams of staff in SIS reveal the existence of an alert issued by a Member State, the	agencies, in particular the European Asylum Support Office and Europol, may also deploy experts as part of migration management support teams, who are not members of the staff of those Union agencies. The objective of the deployment of the, ***as defined in Article 2(8) of Regulation (EU) 2016/1624*** and the migration management support team is to provide for technical and operational reinforcement to the requesting Member States, especially to those facing disproportionate migratory challenges. Fulfilling the tasks assigned to the teams, ***as defined in Article 2(8) of Regulation (EU) 2016/1624*** and the migration management support team necessitates access to SIS via a technical interface of the European Border and Coast Guard Agency connecting to Central SIS. In cases where searches carried out by the team or the teams of staff in SIS reveal the existence of an alert issued by a Member State, the member of the team or the staff cannot take the required action unless authorised to do so by the	border surveillance and return. Other relevant Union agencies, in particular the European Asylum Support Office and Europol, may also deploy experts as part of migration management support teams, who are not members of the staff of those Union agencies. The objective of the deployment of the European Border and Coast Guard teams, teams of staff involved in return-related tasks and the migration management support team**s** is to provide for technical and operational reinforcement to the requesting Member States, especially to those facing disproportionate migratory challenges. Fulfilling the tasks assigned to the European Border and Coast Guard teams, teams of staff involved in return-related tasks and **to** the migration management support team**s** necessitates access to SIS via a technical interface of the European Border and Coast Guard Agency connecting to Central SIS. In cases where searches carried out by the team or the teams of staff in SIS reveal the existence of an alert issued by a Member State, the	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	member of the team or the staff cannot take the required action unless authorised to do so by the host Member State. Therefore it should inform the Member States concerned allowing for follow up of the case.	host Member State. Therefore it should inform the Member States concerned allowing for follow up of the case.	member of the team or the staff cannot take the required action unless authorised to do so by the host Member State. Therefore it should inform the **host** Member States ~~concerned~~ allowing for follow up of the case. **The host Member State should notify the hit to the issuing Member State through the exchange of supplementary information.**	
74	(47) In accordance with Commission proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)[38] the ETIAS Central Unit of the European Border and Coast Guard Agency will perform verifications in SIS via ETIAS in order to perform the assessment of the applications for travel authorisation which require, inter alia, to ascertain if the third country national applying for a travel authorisation is subject of a SIS alert. To this end the ETIAS Central Unit within the European	***[***(47) In accordance with ***[***Regulation **.../...** of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)] the ETIAS Central Unit ***established within*** the European Border and Coast Guard Agency will perform verifications in SIS via ETIAS in order to perform the assessment of the applications for travel authorisation which require, inter alia, to ascertain if the third country national applying for a travel authorisation is subject of a SIS alert. To this end the ETIAS Central Unit within the European	(47) In accordance with Commission proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS)[39] the ETIAS Central Unit of the European Border and Coast Guard Agency will perform verifications in SIS via ETIAS in order to perform the assessment of the applications for travel authorisation which require, inter alia, to ascertain if the third country national applying for a travel authorisation is subject of a SIS alert. To this end the ETIAS Central Unit within the European	*Linked to Art. 49A (agreed to be dropped on 2018-04-13 (DS)).*

38 COM (2016)731 final.
39 COM (2016)731 final.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Border and Coast Guard Agency should also have access to SIS to the extent necessary to carry out its mandate, namely to all alert categories on persons and alerts on blank and issued personal identification documents.	Border and Coast Guard Agency should have access to SIS to the extent ***which is strictly*** necessary to carry out its mandate, namely to all alert categories on third country nationals in respect of whom an alert has been issued for the purposes of entry and stay, and those who are subject to restrictive measure intended to prevent entry or transit through Member States***.]***	Border and Coast Guard Agency should also have access to SIS to the extent necessary to carry out its mandate, namely to all alert categories on persons and alerts on blank and issued personal identification documents.	
75	(48) Owing to their technical nature, level of detail and need for regular updating, certain aspects of SIS cannot be covered exhaustively by the provisions of this Regulation. These include, for example, technical rules on entering data, updating, deleting and searching data, data quality and search rules related to biometric identifiers, rules on compatibility and priority of alerts, the adding of flags, links between alerts, specifying new object categories within the technical and electronic equipment category, setting the expiry date of alerts within the maximum time limit and the exchange of supplementary information. Implementing powers	(48) Owing to their technical nature, level of detail and need for regular updating, certain aspects of SIS cannot be covered exhaustively by the provisions of this Regulation. These include, for example, technical rules on entering data, updating, deleting and searching data, data quality, the adding of flags, links between alerts, specifying new object categories within the technical and electronic equipment category ***and*** setting the expiry date of alerts ***for categories of object alerts*** within the maximum time limit. Implementing powers in respect of those aspects should therefore be conferred to the Commission. Technical rules on searching alerts should take into account the	(48) Owing to their technical nature, level of detail and need for regular updating, certain aspects of SIS cannot be covered exhaustively by the provisions of this Regulation. These include, for example, technical rules on entering data, updating, deleting and searching data, data quality and search rules related to biometric ~~identifiers~~**data**, rules on compatibility and priority of alerts, ~~the adding of flags,~~ links between alerts, specifying new object categories within the technical and electronic equipment category, setting the expiry date of alerts within the maximum time limit and the exchange of supplementary information. Implementing powers	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	in respect of those aspects should therefore be conferred to the Commission. Technical rules on searching alerts should take into account the smooth operation of national applications.	smooth operation of national applications.	in respect of those aspects should therefore be conferred to the Commission. Technical rules on searching alerts should take into account the smooth operation of national applications.	
76		***(48a) The correct application of this Regulation is in the interest of all Member States and necessary to maintain the Schengen area as an area without internal border controls. In order to ensure the correct application of this Regulation by Member States, evaluations conducted through the mechanism established by Regulation (EU) No 1053/2013 are of particular importance. Member States should therefore swiftly address any recommendations made to them. The Commission should, where recommendations are not followed, make use of its powers under the Treaties.***		
77	(49) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with		(49) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Regulation (EU) No 182/2011[40]. The procedure for adopting implementing measures under this Regulation and Regulation (EU) 2018/xxx (border checks) should be the same.		**Article 5 of** Regulation (EU) No 182/2011[41]. The procedure for adopting implementing measures under this Regulation and Regulation (EU) 2018/xxx (border checks) should be the same.	
78	(50) In order to ensure transparency, a report on the technical functioning of Central SIS and the communication infrastructure, including its security, and on the exchange of supplementary information should be produced every two years by the Agency. An overall evaluation should be issued by the Commission every four years.	(50) In order to ensure transparency, a report on the technical functioning of Central SIS and the communication infrastructure, including its security, and on the exchange of supplementary information should be produced ***one year after SIS is brought into operation*** by the Agency. An overall evaluation should be issued by the Commission every ***two*** years.	(50) In order to ensure transparency, a report on the technical functioning of Central SIS and the communication infrastructure, including its security, and on the **bilateral and multilateral** exchange of supplementary information should be produced every two years by the Agency. An overall evaluation should be issued by the Commission every four years.	*Linked to Art. 71.*
79		***(50a) In order to ensure the smooth functioning of SIS, 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 adoption of a manual***		

[40] Regulation (EU) No182/2011 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).

[41] Regulation (EU) No182/2011 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).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		containing detailed rules on the exchange of supplementary information (the SIRENE Manual); ***– rules on logs of automated scanned searches;*** ***– the requirements to be fulfilled for the entering of biometric identifiers into the SIS;*** ***– the adoption of the procedure for designating the Member State responsible for entering an alert on third-country nationals subject to restrictive measures;*** ***– the use of photographs and facial images for the purpose of identifying persons;*** ***– retention periods for categories of object alerts which are shorter than the maximum period of five years; and*** ***– amendments to the date of application of this Regulation.*** ***It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those***		

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[42]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.		
80	(51) Since the objectives of this Regulation, namely the establishment and regulation of a joint information system and the exchange of related supplementary information, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the Treaty of the		(51) Since the objectives of this Regulation, namely the establishment and regulation of a joint information system and the exchange of related supplementary information, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the Treaty of the	

42 ***OJ L 123, 12.5.2016, p. 1.***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.		European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.	
81	(52) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation seeks to ensure a safe environment for all persons residing on the territory of the European Union and special protection for children who could be victim of trafficking or parental abduction while fully respecting the protection of personal data.	(52) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation ***should fully respect the protection of personal data in accordance with Article 8 of the Charter of Fundamental Rights of the European Union while seeking*** to ensure a safe environment for all persons residing on the territory of the European Union and special protection for children who could be victim of trafficking or abduction. ***In cases concerning children, the best interests of the child should be a primary consideration.***	(52) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation seeks to ensure a safe environment for all persons residing on the territory of the European Union and special protection for children who could be victim of trafficking or parental abduction while fully respecting the protection of personal data.	
82	(53) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark annexed to the Treaty on European Union and		(53) In accordance with Articles 1 and 2 of Protocol No 22 on the Position of Denmark annexed to the Treaty on European Union and	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	to the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.		to the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.	
83	(54) The United Kingdom is taking part in this Regulation in accordance with Article 5 of the Protocol on the Schengen acquis integrated into the framework of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union and Article 8(2) of 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		(54) The United Kingdom is taking part in this Regulation in accordance with Article 5**(1)** of ~~the~~ Protocol **No 19** on the Schengen acquis integrated into the framework of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union and Article 8(2) of 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~~	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	some of the provisions of the Schengen acquis[43].		~~some of the provisions of the Schengen acquis~~[44].	
84	(55) Ireland is taking part in this Regulation in accordance with Article 5 of the Protocol on the Schengen acquis integrated into the framework of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union and Article 6(2) of 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[45].		(55) Ireland is taking part in this Regulation in accordance with Article 5 of ~~the~~ Protocol **No 19** on the Schengen acquis integrated into the framework of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union and Article 6(2) of 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~~[46].	
85	(56) As regards Iceland and Norway, this Regulation constitutes a development of 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		(56) As regards Iceland and Norway, this Regulation constitutes a development of 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	

43 OJ L 131, 1.6.2000, p. 43.
44 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).
45 OJ L 64, 7.3.2002, p.20.
46 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).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[47], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC[48]on certain arrangements for the application of that Agreement.		Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[49], which fall within the area referred to in Article 1, point G of Council Decision 1999/437/EC[50]on certain arrangements for the application of that Agreement.	
86	(57) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement signed 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, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 4(1) of		(57) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement ~~signed~~ 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, which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article ~~4(1)~~**3** of	

47 OJ L 176, 10.7.1999, p.36.
48 OJ L 176, 10.7.1999, p.31.
49 OJ L 176, 10.7.1999, p.36.
50 OJ L 176, 10.7.1999, p.31.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Council Decisions 2004/849/EC[51]and 2004/860/EC[52].		Council Decisions~~ 2004/849/EC[53] and 2004/860/EC[54]~~ **2008/149/JHA**[55].	
87	(58) As regards Liechtenstein, this Decision constitutes a development of the provisions of the Schengen acquis 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		(58) As regards Liechtenstein, this Decision constitutes a development of the provisions of the Schengen acquis 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	

51 Council Decision 2004/849/EC of 25 October 2004 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 368, 15.12.2004, p. 26).

52 Council Decision 2004/860/EC of 25 October 2004 on the signing, on behalf of the European Community, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation, concerning the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 370, 17.12.2004, p. 78).

~~53 Council Decision 2004/849/EC of 25 October 2004 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation concerning the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 368, 15.12.2004, p. 26).~~

~~54 Council Decision 2004/860/EC of 25 October 2004 on the signing, on behalf of the European Community, and on the provisional application of certain provisions of the Agreement between the European Union, the European Community and the Swiss Confederation, concerning the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 370, 17.12.2004, p. 78).~~

55 Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of 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 acquis (OJ L 53, 27.2.2008, p. 50).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Confederation's association with the implementation, application and development of the Schengen acquis[56], which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU[57] and Article 3 of Council Decision 2011/350/EU[58].		Confederation's association with the implementation, application and development of the Schengen acquis[59], which fall within the area referred to in Article 1, point G, of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/349/EU[60] ~~and Article 3 of Council Decision 2011/350/EU[61]~~.	
88	(59) As regards Bulgaria and Romania, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen	(59) As regards Bulgaria and Romania, this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within the meaning of	(59) As regards Bulgaria**,** ~~and~~ Romania **and Croatia**, this Regulation constitutes an act building upon, or otherwise	*To be adapted.*

56 OJ L 160, 18.6.2011, p. 21.

57 Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union 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 *acquis*, relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

58 Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, 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 *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

59 OJ L 160, 18.6.2011, p. 21.

60 Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union 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 *acquis*, relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).

61 ~~Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, 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 *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	acquis within the meaning of Article Article 4(2) of the 2005 Act of Accession and should be read in conjunction with Council Decision 2010/365/EU on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania[62].	Article 4(2) of the 2005 Act of Accession and should ***result in the amendment of*** Council Decision 2010/365/EU on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania[63] ***to enable those two Member States to apply and implement the provisions of this Regulation in full***.	relating to, the Schengen acquis within**, respectively,** the meaning of ~~Article~~ Article 4(2) of the 2005 Act of Accession **and Article 4(2) of the 2011 Act of Accession,** and should be read in conjunction with**, respectively,** Council Decision 2010/365/EU on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania[64] **and Council Decision 2017/733 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Croatia**.[65]	
89	(60) Concerning Cyprus and Croatia this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession and Article 4(2) of the 2011 Act of Accession.		(60) Concerning Cyprus ~~and Croatia~~ this Regulation constitutes an act building upon, or otherwise relating to, the Schengen acquis within~~, respectively,~~ the meaning of Article 3(2) of the 2003 Act of Accession ~~and Article 4(2) of the 2011 Act of Accession~~.	

62 OJ L 166, 1.7.2010, p. 17.
63 OJ L 166, 1.7.2010, p. 17.
64 OJ L 166, 1.7.2010, p. 17.
65 OJ L 108, 26.4.20017, p. 31.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
90	(61) This Regulation should apply to Ireland on dates determined in accordance with the procedures set out in the relevant instruments concerning the application of the Schengen acquis to this State.		(61) This Regulation should apply to Ireland on dates determined in accordance with the procedures set out in the relevant instruments concerning the application of the Schengen acquis to this State.	
91	(62) The estimated costs of the upgrade of the SIS national systems and of the implementation of the new functionalities, envisaged in this Regulation are lower than the remaining amount in the budget line for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[66]. Therefore, this Regulation should re-allocate the amount, attributed for developing IT systems supporting the management of migration flows across the external borders.in accordance with Article 5(5)(b) of Regulation (EU) No 515/2014.		~~(62) The estimated costs of the upgrade of the SIS national systems and of the implementation of the new functionalities, envisaged in this Regulation are lower than the remaining amount in the budget line for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[67]. Therefore, this Regulation should re-allocate the amount, attributed for developing IT systems supporting the management of migration flows across the external borders in accordance with Article 5(5)(b) of Regulation (EU) No 515/2014.~~	

[66] 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 (OJ L 150, 20.5.2014, p. 143).

[67] ~~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 (OJ L 150, 20.5.2014, p. 143).~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
92	(63) Council Decision 2007/533/JHA and Commission Decision 2010/261/EU[68] should therefore be repealed.		(63) Council Decision 2007/533/JHA and Commission Decision 2010/261/EU[69] should therefore be repealed.	
93	(64) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on …	(64) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on ***3 May 2017,***	(64) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on …	
94	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	
95	**CHAPTER I**	**CHAPTER I**	**CHAPTER I**	**CHAPTER I**
96	**GENERAL PROVISIONS**	**GENERAL PROVISIONS**	**GENERAL PROVISIONS**	**GENERAL PROVISIONS**
97	*Article 1*	*Article 1*	*Article 1*	*Article 1*
98	*General purpose of SIS*	*General purpose of SIS*	*General purpose of SIS*	*General purpose of SIS*
99	The purpose of SIS shall be to ensure 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 the		The purpose of SIS shall be to ensure 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 the	The purpose of SIS shall be to ensure 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 the

[68] Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (OJ L 112, 5.5.2010, p.31).

[69] Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (OJ L 112, 5.5.2010, p.31).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	safeguarding of security in the territories of the Member States, and to apply the provisions of Chapter 4 and Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union relating to the movement of persons on their territories, using information communicated via this system.		safeguarding of security in the territories of the Member States, and to ~~apply~~**ensure the application of** the provisions of Chapter 4 and Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union relating to the movement of persons on their territories, using information communicated via this system.	safeguarding of security in the territories of the Member States, and to ~~apply~~**ensure the application of** the provisions of Chapter 4 and Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union relating to the movement of persons on their territories, using information communicated via this system.
100	*Article 2*	*Article 2*	*Article 2*	*Article 2*
101	*Scope*	***Subject matter***	*Scope*	***Subject matter***
102	1. This Regulation establishes the conditions and procedures for the entry and processing in SIS of alerts on persons and objects, the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.		1. This Regulation establishes the conditions and procedures for the entry and processing in SIS of alerts on persons and objects, the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.	1. This Regulation establishes the conditions and procedures for the entry and processing in SIS of alerts on persons and objects, the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters.
103	2. This Regulation also lays down provisions on the technical architecture of SIS, the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area		2. This Regulation also lays down provisions on the technical architecture of SIS, the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area	2. This Regulation also lays down provisions on the technical architecture of SIS, the responsibilities of the Member States and of the European Agency for the operational management of large-scale IT systems in the area

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	of freedom, security and justice, general data processing, the rights of the persons concerned and liability.		of freedom, security and justice, general data processing, the rights of the persons concerned and liability.	of freedom, security and justice, general data processing, the rights of the persons concerned and liability.
104	*Article 3*	*Article 3*	*Article 3*	*Article 3*
105	*Definitions*	*Definitions*	*Definitions*	*Definitions* *To be discussed*
106	1. For the purposes of this Regulation, the following definitions shall apply:		1. For the purposes of this Regulation, the following definitions shall apply:	
107	(a) 'alert' means a set of data, including biometric identifiers as referred to in Article 22 and in Article 40, entered in SIS allowing the competent authorities to identify a person or an object with a view to taking specific action;	(a) 'alert' means a set of data entered in SIS allowing the competent authorities to identify a person or an object with a view to taking specific action;	(a) 'alert' means a set of data, including**, where applicable,** biometric ~~identifiers~~ **data** as referred to in Article 22 and in Article 40, entered in SIS allowing the competent authorities to identify a person or an object with a view to taking specific action;	
108	(b) 'supplementary information' means information not forming part of the alert data stored in SIS, but connected	(b) 'supplementary information' means information not forming part of the alert data stored in SIS , but connected to SIS alerts, which is to be exchanged ***by the SIRENE Bureaux***:	(b) 'supplementary information' means information not forming part of the alert data stored in SIS, but connected to SIS alerts, which is to be	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	to SIS alerts, which is to be exchanged:		exchanged **via the SIRENE Bureaux**:	
109	(1) in order to allow Member States to consult or inform each other when entering an alert;		(1) in order to allow Member States to consult or inform each other when entering an alert;	
110	(2) following a hit in order to allow the appropriate action to be taken;		(2) following a hit in order to allow the appropriate action to be taken;	
111	(3) when the required action cannot be taken;		(3) when the required action cannot be taken;	
112	(4) when dealing with the quality of SIS data;		(4) when dealing with the quality of SIS data;	
113	(5) when dealing with the compatibility and priority of alerts;		(5) when dealing with the compatibility and priority of alerts;	
114	(6) when dealing with rights of access;		(6) when dealing with rights of access;	
115	(c) 'additional data' means the data stored in SIS and connected with SIS alerts which are to be immediately available to the competent authorities where a person in respect of whom data has		(c) 'additional data' means the data stored in SIS and connected with SIS alerts which are to be immediately available to the competent authorities where a person in respect of whom data has	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	been entered in SIS is located as a result of searches made therein;		been entered in SIS is located as a result of searches made therein;	
116	(d) 'personal data' means any information relating to an identified or identifiable natural person ('data subject');	(d) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); ***for the purposes of this definition an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;***	(d) 'personal data' means any information relating to an identified or identifiable natural person ('data subject');	
117	(e) 'an identifiable natural person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,	***deleted***	(e) 'an identifiable natural person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	cultural or social identity of that natural person;		cultural or social identity of that natural person;	
118		***(ea) 'alias' means an assumed identity used by a person known under other identities;***		
119	(f) 'processing of personal data' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, logging, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	(f) 'processing of personal data' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, ***recording***, logging, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	(f) 'processing of personal data' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, logging, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	
120	(g) a 'hit' in SIS means:		(g) a '~~hit~~**match**' ~~in SIS~~means **the occurrence of the following steps**:	
121	(1) a search is conducted by a user;		(1) a search is conducted by a**n end-**user;	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
122	(2) the search reveals an alert entered by another Member State in SIS;	(2) the search reveals ***that*** an alert ***is*** entered by ***a*** Member State in SIS;	(2) the search reveals an alert entered by another Member State in SIS; **and**	
123	(3) data concerning the alert in SIS match the search data; and		(3) data concerning the alert in SIS match the search data**.**~~; and~~	
124			**(ga) a 'hit' means any match which fulfils the following criteria:**	
125			**(a) it has been confirmed:**	
126			**(i) by the end-user, or**	
127			**(ii)where the match concerned was based on the comparison of biometric data by the competent authority in accordance with national procedures;**	
128			**and**	
129	(4) further actions are requested.		(4**b**) further actions are requested.	
130	(h) 'flag' means a suspension of validity of an alert at the		(h) 'flag' means a suspension of validity of an alert at the	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	national level that may be added to alerts for arrest, alerts for missing persons and alerts for discreet, inquiry and specific checks, where a Member State considers that to give effect to an alert is incompatible with its national law, its international obligations or essential national interests. Where the alert is flagged, the requested action on the basis of the alert shall not be taken on the territory of this Member State.		national level that may be added to alerts for arrest, alerts for missing **and vulnerable** persons and alerts for discreet, inquiry and specific checks~~, where a Member State considers that to give effect to an alert is incompatible with its national law, its international obligations or essential national interests. Where the alert is flagged, the requested action on the basis of the alert shall not be taken on the territory of this Member State.~~**;**	
131	(i) 'issuing Member State' means the Member State which entered the alert in SIS;		(i) 'issuing Member State' means the Member State which entered the alert in SIS;	
132	(j) 'executing Member State' means the Member State which takes or has taken the required actions following a hit;		(j) 'executing Member State' means the Member State which takes or has taken the required actions following a hit;	
133	(k) 'end-users' mean competent authorities directly searching		(k) 'end-users' mean competent authorities directly searching	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	CS-SIS, N.SIS or a technical copy thereof;		CS-SIS, N.SIS or a technical copy thereof;	
134		***(ka) 'biometric identifiers' means personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person, which allow or confirm the unique identification of that natural person (facial images, dactyloscopic data and DNA profile);***	**(ka) 'biometric data' means biometric data as defined in Article 3(13) of Directive (EU) 2016/680;**	
135	(l) 'dactylographic data' means data on fingerprints and palm prints which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;	(l) '***dactyloscopic*** data' means data on fingerprints and palm prints which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;	(l) 'dactylo~~graphic~~**scopic**data' means ~~data on~~ fingerprints **images, images of fingerprint latents** ~~and~~ palm prints**, palm prints latents and templates of such images (coded minutiae)** [70] which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity;	
136		***(la) 'facial image' means digital images of the face with a sufficient image resolution and***	**(la) 'facial image' means digital images of the face with sufficient image resolution**	

[70] Same definition as in Council Decision 2008/616/JHA.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		quality to be used in automated biometric matching;	**and quality to be used in automated biometric matching;** [71]	
137		***(lb) 'DNA profile' means a letter or number code which represents a set of identification characteristics of the noncoding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci);***	**(lb) 'DNA profile' means a letter or number code which represents a set of identification characteristics of the noncoding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci)** [72]**;**	
138	(m) 'serious crime' means offences listed in Article 2(1) and (2) of Framework Decision 2002/584/JHA of 13 June 2002[73];	***deleted***	(m) 'serious crime' means offences listed in Article 2(1) and (2) of Framework Decision 2002/584/JHA of 13 June 2002; [74]	*Rapporteur's informal proposal* **Deletion**
139	(n) 'terrorist offences' means offences under national law referred to in Articles 1-4 of	(n) 'terrorist offences' means offences under national law referred to in Articles ***3 to 12 and***	(n) 'terrorist offences' means **an** offences under national law **which corresponds or is**	

[71] Same definition as in the EES proposal (see Article 3(16) in 11037/17 + ADD 1 +ADD 2).

[72] Same definition as in Article 2(c) of Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

[73] Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.07.2002, p. 1).

[74] Council Framework Decision (2002/584/JHA) of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.07.2002, p. 1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Framework Decision 2002/475/JHA of 13 June 2002[75].	***14 of Directive (EU) 2017/541***.	**equivalent to one of the offences** referred to in ~~Articles 1-4of Framework Decision 2002/475/JHA of 13 June 2002[76].~~**Directive (EU) 2017/541**[77].	
140			**(o) 'vulnerable persons' means persons who, due to their age, physical or mental state, or due to their social or family circumstances, require protection.**	*Rapporteur's informal proposal* **Deletion**
141			**(p) 'threat to public health' means threat to public health as defined by Regulation (EU) 2016/399[78].**	
142	*Article 4*	*Article 4*	*Article 4*	*Article 4*
143	*Technical architecture and ways of operating SIS*	*Technical architecture and ways of operating SIS*	*Technical architecture and ways of operating SIS*	*Technical architecture and ways of operating SIS*

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

~~76 Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).~~

77 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31/03/2017, p. 6.

78 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 (Schengen Borders Code);

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				Provisionaly agreed at political level on trilogue on 7 February 2018, subject to further refinement at technical level.
144	1. SIS shall be composed of:		1. SIS shall be composed of:	1. SIS shall be composed of:
145	(a) a central system (Central SIS) composed of:		(a) a central system (Central SIS) composed of:	(a) a central system (Central SIS) composed of:
146	– a technical support function ('CS-SIS') containing a database, the 'SIS database',		– a technical support function ('CS-SIS') containing a database, the 'SIS database',	- a technical support function ('CS-SIS') containing a database, the 'SIS database',
147	– a uniform national interface (NI-SIS);		– a uniform national interface (NI-SIS);	- a uniform national interface (NI-SIS);
148	(b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS shall contain a data file (a 'national copy'), containing a complete or partial copy of the SIS database as well as a backup N.SIS. The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users;	(b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS ***may*** contain a data file (a 'national copy'), containing a complete or partial copy of the SIS database as well as a backup N.SIS. The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users;	(b) a national system (N.SIS) in each of the Member States, consisting of the national data systems which communicate with Central SIS. An N.SIS ~~shall~~**may** contain a data file (a 'national copy'), containing a complete or partial copy of the SIS database ~~as well as a backup N.SIS~~. **Two or more Member States may establish in one of their N.SIS a shared copy which may be used jointly by these Member States. Such**	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			shared copy shall be considered as the national copy of each of the participating Member States;	
a.			**(ba) at least one national or shared backup site in each N.SIS. A shared backup N.SIS may be used jointly by two or more Member States and shall be considered as the back-up N.SIS of each of the participating Member States**. The N.SIS and its backup may be used simultaneously to ensure uninterrupted availability to end-users; **and**	
149	(c) a communication infrastructure between CS-SIS and NI-SIS (the Communication Infrastructure) that provides an encrypted virtual network dedicated to SIS data and the exchange of data between		(c) a communication infrastructure between CS-SIS and NI-SIS (the Communication Infrastructure) that provides an encrypted virtual network dedicated to SIS data and the exchange of data between	Commission services proposal, that could be acceptable for the Council: (c) a communication infrastructure between CS-SIS, ***backup CS-SIS*** and NI-SIS (the Communication Infrastructure) that provides an encrypted virtual network dedicated to SIS data and the exchange of data between SIRENE Bureaux as referred to in Article 7(2).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	SIRENE Bureaux as referred to in Article 7(2).		SIRENE Bureaux as referred to in Article 7(2).	EP addition introduced in the trilogue of 7 February is acceptable for the Council: ***Member States intending to establish a shared copy or shared backup site to be used jointly shall agree their respective responsibilities in writing. They shall notify this arrangement to the Commission.***
150		***A backup communication infrastructure shall be developed to further ensure the uninterrupted availability of SIS. Detailed rules for this backup communication infrastructure shall be adopted by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).***		Commission services proposal of 9 January with the EP adjustments from 7 February is acceptable for the Council: ***The communication infrastructure shall ~~be developed to~~ support and contribute to ensuring the uninterrupted availability of SIS. It shall include redundant and separated paths for the connections between CS-SIS and the backup CS-SIS and shall also include redundant and separated paths for the connections between each SIS national network access point and CS-SIS and backup CS-SIS.***
151				2. ~~SIS data~~ **Member States** shall ~~be~~ entere~~d~~, update~~d~~, delete~~d~~ and search~~ed~~ **SIS data** via the various N.SIS. A partial or a full national [**or**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	2. SIS data shall be entered, updated, deleted and searched via the various N.SIS. A partial or a full national copy shall be available for the purpose of carrying out automated searches in the territory of each of the Member States using such a copy. The partial national copy shall contain at least the data listed in Article 20 (2) concerning objects and the data listed in Article 20(3) (a) to (v) of this Regulation concerning alerts on persons. It shall not be possible to search the data files of other Member States' N.SIS.	2. SIS data shall be entered, updated, deleted and searched via the various N.SIS.	2. ~~SIS data~~**Member States** shall ~~be~~ entere~~d~~, update~~d~~, delete~~d~~ and search~~ed~~ **SIS data** via the various N.SIS. A partial or a full national **or shared** copy shall be available for the purpose of carrying out automated searches in the territory of each of the Member States using such a copy. The partial national **or shared** copy shall contain at least the data listed in Article 20(2) concerning objects and the data listed in Article 20(3) (a) to (v) **and (z)** of this Regulation concerning alerts on persons. It shall not be possible to search the data files of other Member States' N.SIS.	**shared]** copy shall be available for the purpose of carrying out automated searches in the territory of each of the Member States using such a copy. The partial national **[or shared]** copy shall contain at least the data listed in Article 20(2) (a) **to** (v) of this Regulation. It shall not be possible to search the data files of other Member States' N.SIS.
152	3. CS-SIS shall perform technical supervision and administration functions and have a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of this system. CS-SIS and the backup CS-SIS shall be located in the two technical sites of the European Agency for the operational management of large-scale information systems in the area of freedom, security and	3. CS-SIS shall perform technical supervision and administration functions and have a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of this system. CS-SIS and the backup CS-SIS shall be located in the two technical sites of the European Agency for the operational management of large-scale information systems in the area of freedom, security and justice established by Regulation	3. CS-SIS shall perform technical supervision and administration functions and have a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of this system. **CS-SIS and the backup CS-SIS may operate simultaneously.** CS-SIS and the backup CS-SIS shall be located in the ~~two~~ technical sites of the European Agency for the operational management of large-	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	justice established by Regulation (EU) No 1077/2011[79]('the Agency'). CS-SIS or backup CS-SIS may contain an additional copy of the SIS database and may be used simultaneously in active operation provided that each of them is capable to process all transactions related to SIS alerts.	(EU) No 1077/2011[80] ('the Agency'). CS-SIS or backup CS-SIS ***shall*** contain an additional copy of the SIS database and ***shall*** be used simultaneously in active operation provided that each of them is capable to process all transactions related to SIS alerts.	scale information systems in the area of freedom, security and justice established by Regulation (EU) No 1077/2011 ('the Agency'). CS-SIS or backup CS-SIS may contain ~~an additional~~ **technical** copy of the SIS database ~~and~~ **which** may be used simultaneously**,** ~~in active operation~~ provided that each of them is capable to process all transactions related to SIS alerts.	
153	4. CS-SIS shall provide the services necessary for the entry and processing of SIS data, including searches in the SIS database. CS-SIS shall:	4. CS-SIS shall provide the services necessary for the entry and processing of SIS data, including searches in the SIS database. ***For the Member States which use a national copy,*** CS-SIS shall:	4. CS-SIS shall provide the services necessary for the entry and processing of SIS data, including searches in the SIS database. CS-SIS shall:	4. CS-SIS shall provide the services necessary for the entry and processing of SIS data, including searches in the SIS database. ***For the Member States which use a national [or shared] copy,*** CS-SIS shall:
154	(a) provide online update of the national copies;		(a) provide online update of the national copies;	(a) provide online update of the national copies;
155	(b) ensure synchronisation of and consistency between the national copies and the SIS database;		(b) ensure synchronisation of and consistency between the national copies and the SIS database;	(b) ensure synchronisation of and consistency between the national copies and the SIS database; and

[79] Established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

[80] Established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 286, 1.11.2011, p.1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
156	(c) provide the operation for initialisation and restoration of the national copies;		(c) provide the operation for initialisation and restoration of the national copies; **and**	(c) provide the operation for initialisation and restoration of the national copies;
157	(d) provide uninterrupted availability.		(d) provide uninterrupted availability.	CS-SIS shall provide uninterrupted availability.
158	*Article 5*		*Article 5*	*Article 5*
159	*Costs*		*Costs*	*Costs*
160	1. The costs of operating, maintaining and further developing Central SIS and the Communication Infrastructure shall be borne by the general budget of the European Union.		1. The costs of operating, maintaining and further developing Central SIS and the Communication Infrastructure shall be borne by the general budget of the European Union.	1. The costs of operating, maintaining and further developing Central SIS and the Communication Infrastructure shall be borne by the general budget of the European Union.
161	2. These costs shall include work done with respect to CS-SIS that ensures the provision of the services referred to in Article 4(4).		2. These costs shall include work done with respect to CS-SIS that ensures the provision of the services referred to in Article 4(4).	2. These costs shall include work done with respect to CS-SIS that ensures the provision of the services referred to in Article 4(4).
162	3. The costs of setting up, operating, maintaining and further developing each N.SIS shall be borne by the Member State concerned.		3. The costs of setting up, operating, maintaining and further developing each N.SIS shall be borne by the Member State concerned.	3. The costs of setting up, operating, maintaining and further developing each N.SIS shall be borne by the Member State concerned.
163	**CHAPTER II**	**CHAPTER II**	**CHAPTER II**	**CHAPTER II**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
164	**RESPONSIBILITIES OF THE MEMBER STATES**	**RESPONSIBILITIES OF THE MEMBER STATES**	**RESPONSIBILITIES OF THE MEMBER STATES**	**RESPONSIBILITIES OF THE MEMBER STATES**
165	*Article 6*	*Article 6*	*Article 6*	*Article 6*
166	*National systems*	*National systems*	*National systems*	*National systems* To be finalised in the context of Architecture.
167	Each Member State shall be responsible for setting up, operating, maintaining and further developing its N.SIS and connecting its N.SIS to NI-SIS.		Each Member State shall be responsible for setting up, operating, maintaining and further developing its N.SIS and connecting its N.SIS to NI-SIS.	Each Member State shall be responsible for setting up, operating, maintaining and further developing its N.SIS and connecting its N.SIS to NI-SIS.
168	Each Member State shall be responsible for ensuring the continuous operation of the N.SIS, its connection to NI-SIS and the uninterrupted availability of SIS data to the end-users.	Each Member State shall be responsible for ensuring the continuous operation of the N.SIS ***and*** its connection to NI-SIS.	Each Member State shall be responsible for ensuring the continuous operation of the N.SIS, its connection to NI-SIS and the uninterrupted availability of SIS data to the end-users.	Commission services proposal is to delete, which can be acceptable for the Council.
169		***Each Member State shall be responsible for ensuring the uninterrupted availability of SIS data to end-users, in particular by establishing a duplicate connection with NI-SIS.***		Commission services proposal: ***Each Member State shall be responsible for ensuring the uninterrupted availability of SIS data to end-users~~, in particular by establishing~~ and establish a duplicate connection of CS-SIS with NI-SIS.*** Acceptable for LIBE Latest Commission services proposal

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				of 9 January is to stop the sentence after end-users. This would be acceptable for the Council.
170			**Each Member State shall transmit its alerts via its N.SIS**[81].	**Each Member State shall transmit its alerts via its N.SIS.**
171	*Article 7*	*Article 7*	*Article 7*	*Article 7*
172	*N.SIS Office and SIRENE Bureau*	*N.SIS Office and SIRENE Bureau*	*N.SIS Office and SIRENE Bureau*	*N.SIS Office and SIRENE Bureau*
173	1. Each Member State shall designate an authority (the N.SIS Office), which shall have central responsibility for its N.SIS.		1. Each Member State shall designate an authority (the N.SIS Office), which shall have central responsibility for its N.SIS.	1. Each Member State shall designate an authority (the N.SIS Office), which shall have central responsibility for its N.SIS.
174	That authority shall be responsible for the smooth operation and security of the N.SIS, shall ensure the access of the competent authorities to the SIS and shall take the necessary measures to ensure compliance with the provisions of this Regulation. It shall be responsible for ensuring that all functionalities of SIS are appropriately made available to the end users.		That authority shall be responsible for the smooth operation and security of the N.SIS, shall ensure the access of the competent authorities to the SIS and shall take the necessary measures to ensure compliance with the provisions of this Regulation. It shall be responsible for ensuring that all functionalities of SIS are appropriately made available to the end users.	That authority shall be responsible for the smooth operation and security of the N.SIS, shall ensure the access of the competent authorities to the SIS and shall take the necessary measures to ensure compliance with the provisions of this Regulation. It shall be responsible for ensuring that all functionalities of SIS are appropriately made available to the end users.

[81] Moved from Article 7(1) *in fine*, excluding the word 'Office' at the end of the sentence.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
175	Each Member State shall transmit its alerts via its N.SIS Office.	Each Member State shall ***enter alerts on the basis of all available information falling under the scope of this Regulation, and shall*** transmit its alerts via its N.SIS Office.	~~Each Member State shall transmit its alerts via its N.SIS Office.~~[82]	LIBE withdraws AM ~~Each Member State shall transmit its alerts via its N.SIS Office.~~[83]
176	2. Each Member State shall designate the authority which shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8.	2. Each Member State shall designate ***a national*** authority which ***is operational 24 hours a day, 7 days a week and*** shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8. ***The SIRENE Bureau shall serve as the sole point of contact to Member States for the exchange of supplementary information on alerts and to make it possible for the appropriate measures to be adopted when alerts on persons and objects have been entered in SIS and those persons and objects are found following a hit.***	2. Each Member State shall designate the authority which shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8.	Council to check LIBE amendment. Commission services proposed: Each Member State shall designate ***a national authority which is operational 24 hours a day, 7 days a week and*** shall ensure the exchange and availability of all supplementary information (the SIRENE Bureau) in accordance with the provisions of the SIRENE Manual, as referred to in Article 8. ***The SIRENE Bureau shall serve as single contact point for Member States to exchange supplementary information regarding alerts and ~~to enable appropriate measures~~ to facilitate the requested actions to be taken when alerts on persons or objects have been entered in SIS and those persons or objects are ~~found~~ located following a hit.*** Commission proposal acceptable for LIBE

[82] Moved to Art. 6 *in fine*.
[83] Moved to Art. 6 *in fine*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				New subparagraph proposal - text from point 1.9.4 SIRENE Manual (2018-03-26) ***In order to fulfil the requirement to provide supplementary information, the SIRENE Bureau staff shall have direct or indirect access to all relevant national information, including national databases and relevant information on its own alerts, and expert advice.*** New subparagraph proposal - text from point 1.16 SIRENE Manual (2018-03-26) ***The SIRENE Bureau of the issuing Member State shall keep all information on its own alerts to be able to react to request for supplementary information swiftly and within the deadline provided for in Article 8.***
177	Those Bureaux shall also coordinate the verification of the quality of the information entered in SIS. For those purposes they		Those Bureaux shall also coordinate the verification of the quality of the information entered in SIS. For those purposes they shall	Those Bureaux shall also coordinate the verification of the quality of the information entered in SIS. For those purposes they shall have access to data processed in SIS.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	shall have access to data processed in SIS.		have access to data processed in SIS.	
178	3. The Member States shall inform the Agency of their N.SIS II office and of their SIRENE Bureau. The Agency shall publish the list of them together with the list referred to in Article 53(8).		3. The Member States shall inform the Agency of their N.SIS ~~II~~ **O**ffice and of their SIRENE Bureau. The Agency shall publish the list of them together with the list referred to in Article 53(8).	3. The Member States shall inform the Agency of their N.SIS ~~II~~ Office and of their SIRENE Bureau. The Agency shall publish the list of them together with the list referred to in Article 36(8).
179	*Article 8*	*Article 8*	*Article 8*	*Article 8*
180	*Exchange of supplementary information*	*Exchange of supplementary information*	*Exchange of supplementary information*	*Exchange of supplementary information*
181	1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Member States shall provide the necessary technical and personal resources to ensure the continuous availability and exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States may use other adequately secured technical means to exchange supplementary information.	1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Member States shall provide the necessary technical and ***human*** resources to ensure the continuous availability and ***timely and effective*** exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States ***shall*** use ***the backup communication infrastructure referred to in***	1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Member States shall provide the necessary technical and ~~personal~~ **human** resources to ensure the continuous availability and exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States may use other adequately secured technical means to exchange supplementary information.	Commission services proposal of 9 January: 1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Member States shall provide the necessary technical and ***human*** resources to ensure the continuous availability and ***timely and effective*** exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States ***shall use ~~the backup communication infrastructure referred to in Article 4(1)(c). As a last resort~~*** other

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		Article 4(1)(c). As a last resort other adequately secured technical means to exchange supplementary information***, such as SIENA, may be used***.		adequately secured technical means to exchange supplementary information***, such as SIENA, may be used***. Can be acceptable for the Council with the deletion of the last phrase (reference to Siena and "may be used" - latter being a mistake. Proposal is acceptable to LIBE with sentence ending after "exchange supplementary information" and by adding: A list of adequately secured technical means shall be laid down in the Sirene Manual. Presidency proposal 03.04.2018 1. Supplementary information shall be exchanged in accordance with the provisions of the SIRENE Manual and using the Communication Infrastructure. Member States shall provide the necessary technical and ***human*** resources to ensure the continuous availability and ***timely and effective*** exchange of supplementary information. In the event that the Communication Infrastructure is unavailable, Member States ***shall use ~~the backup communication infrastructure referred to in~~***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				~~***Article 4(1)(c). As a last resort***~~ other adequately secured technical means, A list of adequately secured technical means shall be laid down in the SIRENE Manual. LIBE to provide feedback
182	2. Supplementary information shall be used only for the purpose for which it was transmitted in accordance with Article 61 unless prior consent is obtained from the issuing Member State.	2. Supplementary information shall be used only for the purpose for which it was transmitted in accordance with Article 61.	2. Supplementary information shall be used only for the purpose for which it was transmitted in accordance with Article 61 unless prior consent is obtained from the issuing Member State.	2. Supplementary information shall be used only for the purpose for which it was transmitted in accordance with Article 61.
183	3. The SIRENE Bureaux shall carry out their task in a quick and efficient manner, in particular by replying to a request as soon as possible but not later than 12 hours after the receipt of the request.	3. The SIRENE Bureaux shall carry out their task in a quick and efficient manner, in particular by ***substantially*** replying to a request ***for supplementary information*** as soon as possible but not later than ***six*** hours after the receipt of the request. ***In cases of alerts for terrorist offences and in cases of alerts concerning children referred to in Article 32(2)(c) the SIRENE Bureaux shall act immediately.***	3. The SIRENE Bureaux shall carry out their task in a quick and efficient manner, in particular by ~~replying~~**reacting** to a request as soon as possible but **preferably** not later than 12 hours after the receipt of the request.	3. The SIRENE Bureaux shall carry out their task in a quick and efficient manner, in particular by replying to a request ***for supplementary information*** as soon as possible but not later than 12 hours after the receipt of the request. ***In case of alerts for terrorist offences, of alerts for persons wanted for arrest for surrender or extradition purposes, and in cases of alerts concerning children referred to in Article 32(2)(c) the SIRENE Bureaux shall act immediately.***
184		***3a. SIRENE forms to be dealt with by the requested SIRENE***		3a. Requests for supplementary Information ***with highest priority***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		Bureau with highest priority may be marked 'URGENT', in the SIRENE forms and the reason for urgency specified.		shall ***be marked 'URGENT', in the SIRENE forms, and the reason for urgency*** shall be ***specified.***
185	4. Detailed rules for the exchange of supplementary information shall be adopted by means of implementing measures in accordance with the examination procedure referred to in Article 72(2) in the form of a manual called the 'SIRENE Manual'.	4. ***The Commission*** shall be ***empowered to adopt a delegated act*** in accordance with Article ***71a concerning the adoption*** of a manual ***containing detailed rules for the exchange of supplementary information (SIRENE Manual)***.	4. **The Commission shall adopt implementing acts to lay down d**etailed rules for the exchange of supplementary information **in the form of a manual entitled the 'SIRENE Manual'. Those implementing acts** shall be adopted ~~by means of implementing measures~~ in accordance with the examination procedure referred to in Article 72(2) ~~in the form of a manual called the 'SIRENE Manual'~~**.**	LIBE maintains its position To be further discussed at technical level, in order to identify elements of the SIRENE Manual to be included in the basic act
186	*Article 9*	*Article 9*	*Article 9*	*Article 9*
187	*Technical and functional compliance*	*Technical and functional compliance*	*Technical and functional compliance*	*Technical and functional compliance*
188	1. When setting up its N.SIS, each Member State shall comply with common standards, protocols and technical procedures established to ensure the compatibility of its N-SIS with CS-SIS for the prompt and effective		1. When setting up its N.SIS, each Member State shall comply with common standards, protocols and technical procedures established to ensure the compatibility of its N-**.**SIS with CS-SIS for the prompt and	1. When setting up its N.SIS, each Member State shall comply with common standards, protocols and technical procedures established to ensure the compatibility of its N**.**-SIS with CS-SIS for the prompt and effective transmission of data.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	transmission of data. Those common standards, protocols and technical procedures shall be adopted by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).		effective transmission of data. ~~Those common standards, protocols and technical procedures shall be adopted by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[84]	~~Those common standards, protocols and technical procedures shall be adopted by means of implementing measures in accordance with the examination procedure referred to in Article 55(2).~~
189	2. Member States shall ensure, by means of the services provided by CS-SIS, that data stored in the national copy are, by means of automatic updates referred to in Article 4(4), identical to and consistent with the SIS database, and that a search in its national copy produces a result equivalent to that of a search in the SIS database. End-users shall receive the data required to perform their tasks, in particular all data required for the identification of the data subject and to take the required action.	2. Member States shall ensure, by means of the services provided by CS-SIS, that data stored in the national copy ***established voluntarily by a Member State,*** are by means of automatic updates referred to in Article 4(4), identical to and consistent with the SIS database, and that a search in its ***voluntary*** national copy produces a result equivalent to that of a search in the SIS database. ***In so far as this is possible,*** end-users shall receive the data required to perform their tasks, in particular***, where necessary, all available data allowing*** for the identification of the data subject and the required action ***to be taken***.	2. Member States shall ensure, by means of the services provided by CS-SIS, that data stored in the national **or shared** copy are, by means of automatic updates referred to in Article 4(4), identical to and consistent with the SIS database, and that a search in its national **or shared** copy produces a result equivalent to that of a search in the SIS database. End-users shall receive the data required to perform their tasks, in particular all data required for the identification of the data subject and to take the required action.	2. Member States shall ensure, by means of the services provided by CS-SIS ***and by means of automatic updates referred to in Article 4(4)*** that ***the*** data stored in the national copy ***are ~~established voluntarily by a Member State, are~~*** ~~by means of automatic updates referred to in Article 4(4)~~ ***are*** identical to and consistent with the SIS database, and that a search in its ***~~voluntary~~*** national copy produces a result equivalent to that of a search in the SIS database. ***~~In so far as this is possible~~.*** ***2a***. End-users shall receive the data required, to perform their tasks, in particular ***and where necessary, all the available data allowing*** for the identification of the data subject and the required action ***to be taken***.

[84] Moved to paragraph 3.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
190		***2a. Regular tests shall be undertaken as part of the mechanism established by Regulation (EU) No 1053/2013 to verify the technical and functional compliance of national copies and, in particular, whether searches in the national copy produce results equivalent to those of a search in SIS.***		***2b. Member States and the Agency shall undertake regular tests to verify the technical compliance of the national copies referred to in paragraph 2. The results of these tests shall be taken into consideration as part of the mechanism established by Regulation (EU) No 1053/2013.***
191			**3.[85] The Commission shall adopt implementing acts to lay down and develop common standards, protocols and technical procedures, referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**	**3. The Commission shall adopt implementing acts to lay down and develop common Standards, protocols and technical procedures, referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**
192	*Article 10*	*Article 10*	*Article 10*	*Article 10*
193	*Security – Member States*	*Security – Member States*	*Security – Member States*	*Security – Member States*
194	1. Each Member State shall, in relation to its N.SIS, adopt the necessary measures, including a		1. Each Member State shall, in relation to its N.SIS, adopt the necessary measures, including a	1. Each Member State shall, in relation to its N.SIS, adopt the necessary measures, including a

[85] Moved from paragraph 1, *in fine*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	security plan, a business continuity plan and a disaster recovery plan in order to:		security plan, a business continuity plan and a disaster recovery plan in order to:	security plan, a business continuity plan and a disaster recovery plan in order to:
195	(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;
196	(b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);	(b) deny unauthorised persons access to data-processing ***equipment and*** facilities used for processing personal data (***equipment,*** access control ***and facilities entry control***);	(b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);	LIBE maintains its position Follows Eurodac proposal of the Commission Similar wording in EES (Art. 43(2)(b)) Council's compromise 03.04.2018 (b) deny unauthorised persons access to data-processing ***equipment and*** facilities used for processing personal data (***equipment,*** access control ***and facilities entry control***);
197	(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);		(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);	(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
198	(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of		(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of	(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	stored personal data (storage control);		stored personal data (storage control);	stored personal data (storage control);
199	(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);		(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);	(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);
200		***(ea) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry);***		LIBE maintains its position Follows Eurodac proposal of the Commission Agreed in EES (Art. 43(2)(f))
201	(f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);		(f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation, by means of individual and unique user ~~identities~~ **identifiers**[86] and confidential access modes only (data access control);	
202	(g) ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles	(g) ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles describing the functions	(g) ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles	LIBE maintains its position

[86] Same wording as in Article 12(2) and (3) and Article 18(2) and (3).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 66 without delay upon their request (personnel profiles);	and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 66 ***immediately*** upon their request (personnel profiles);	describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities referred to in Article 6~~6~~7 without delay upon their request (personnel profiles);	
203	(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);		(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);	(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
204	(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose the data were input (input control);		(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose the data were input (input control);	(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose the data were input (input control);
205	(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers		(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers	(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	of personal data or during transportation of data media, in particular by means of appropriate encryption techniques (transport control);		of personal data or during transportation of data media, in particular by means of appropriate encryption techniques (transport control); **and**	of personal data or during transportation of data media, in particular by means of appropriate encryption techniques (transport control); **and**
206	(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring (self-auditing).		(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring (self-auditing).	(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring (self-auditing).
207		***(ka) ensure that the installed system may, in case of interruption, be restored (recovery);***		LIBE maintains its position Follows Eurodac proposal of the Commission Similar wording in EES (Art. 43(2)(l))
208		***(kb) ensure that SIS performs its functions correctly, that faults are reported (reliability) and that personal data stored in SIS cannot be corrupted by means of a system malfunctioning (integrity);***		LIBE maintains its position Follows Eurodac proposal of the Commission Similar wording in EES (Art. 43(2)(m))
209	2. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the		2. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the	2. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	processing and exchange of supplementary information, including securing the premises of the SIRENE Bureau.		processing and exchange of supplementary information, including securing the premises of the SIRENE Bureau.	processing and exchange of supplementary information, including securing the premises of the SIRENE Bureau.
210	3. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing of SIS data by the authorities referred to in Article 43.		3. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing of SIS data by the authorities referred to in Article 43.	3. Member States shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing of SIS data by the authorities referred to in Article 43.
211			**4. The measures described in paragraphs 1 to 3 may be part of a generic security approach and plan at national level. However, the requirements of this Article and its applicability to the SIS shall be clearly identifiable in and ensured by that plan.**	4. The measures described in paragraphs 1 to 3 may be part of a generic security approach and plan at national level **encompassing multiple IT-systems**. However, the requirements foreseen in this Article and its applicability to the SIS shall be clearly identifiable in and ensured by that plan.
212	*Article 11*	*Article 11*	*Article 11*	*Article 11*
213	*Confidentiality – Member States*	*Confidentiality – Member States*	*Confidentiality – Member States*	*Confidentiality – Member States*
214	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 and supplementary information, in accordance with its		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 and supplementary information, in accordance with its	**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 and supplementary information, in accordance with its

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.		national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.	national law. That obligation shall also apply after those persons leave office or employment or after the termination of the activities of those bodies.
215		***1a. Where a Member State cooperates with external contractors in any SIS-related tasks, that Member State shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.***		***~~2a.~~ Where a Member State cooperates with external contractors in any SIS-related tasks, that Member State shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.*** 3. The operational management of N.SIS or of any technical copies shall not be entrusted to private companies or private organisations.
216	*Article 12*	*Article 12*	*Article 12*	*Article 12*
217	*Keeping of logs at national level*	*Keeping of logs at national level*	*Keeping of logs at national level*	*Keeping of logs at national level*
218	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 whether or not the search is lawful,	1. ***Without prejudice to Article 25 of Directive (EU) 2016/680,*** Member States shall ensure that every access to and all exchanges of personal data within CS-SIS are logged in their N.SIS	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 whether or not the search is lawful,	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 whether or not the search is lawful,

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of N.SIS , data integrity and security.	for the purposes of 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.	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).**	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).**
219	2. The records shall show, in particular, the history of the alert, the date and time of the data processing activity, the data used to perform a search, a reference to the data transmitted and the names of both the competent authority and the person responsible for processing the data.	2. The ***logs*** shall show, in particular, the history of the alert, the date and time of the data processing activity, the ***type of*** data used to perform a search, the data ***processed*** and the ***name*** of both the competent authority and the person ***performing a search and*** processing the data.	2. The ~~records~~ **logs** shall show, in particular, the history of the alert, the date and time of the data processing activity, the data used to perform a search, a reference to the data transmitted and the ~~names~~ **individual and unique user identifiers**[87] of both the competent authority and the person responsible for processing the data.	Commission services proposal of 12 Jan 2018: 2. The logs shall show, in particular, the history of the alert, the date and time of the data processing activity, the ~~type of~~ data used to perform a search, **a reference to the** data ***processed*** and ~~***both***~~ the ~~name~~ **individual and unique user identifiers**[88] of **both** the competent authority and the person ~~***performing a search and***~~ processing the data. LIBE to check
220	3. If the search is carried out with dactylographic data or facial image in accordance with Articles 40, 41 and 42 the logs shall show, in particular, the type of data used to perform a search, a reference to the type of data transmitted and the	3. ***By way of derogation from paragraph 2, if*** the search is carried out with ***dactiloscopic*** data or facial image in accordance with Articles 40, 41 and 42 the logs shall show, the type of data ***processed instead of the actual***	3. If the search is carried out with dactylo~~graphic~~**scopic** data or facial image in accordance with Article~~s 40, 41 and~~ 42 the logs shall show, in particular, the type of data used to perform a search, a reference to the type of data	Commission services proposal of 12 Jan 2018: 3. ***By way of derogation from paragraph 2, if*** the search is carried out with ***dactyloscopic*** data or facial image in accordance with Article 22 the logs shall show the type of data

[87] Same wording as in paragraph 3 and Article 10(1)(f).

[88] Same wording as in paragraph 3 and Article 10(1)(f).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	names of both the competent authority and the person responsible for processing the data.	***data.***	transmitted and the ~~names~~ **individual and unique user identifiers**[89] of both the competent authority and the person responsible for processing the data.	**used to perform the search** ***~~processed~~ instead of*** the ***actual*** data. **The logs shall also contain a reference to the type of data processed and the individual and unique user identifiers of both the competent authority and the person processing the data.** LIBE to check
221		***3a. Rules and formats for logs including regarding the retention period for logs, in order to ensure that the rights of citizens are upheld when it comes to verifying the legality of data processing, and to achieve greater harmonisation of the retention period between Member States and differentiation between the retention period for logs on systematic consultations, particularly at border posts, and other consultations, particularly on the basis of police checks, shall be laid down by means of implementing measures in accordance with the examination procedure referred to in Article***		As part of an overall compromise, could be withdrawn. To be checked, as EP AM differs from Borders proposal: ***<<including regarding the retention period for logs, in order to ensure that the rights of citizens are upheld when it comes to verifying the legality of data processing, and to achieve greater harmonisation of the retention period between Member States and differentiation between the retention period for logs on systematic consultations, particularly at border posts, and***

[89] Same wording as in paragraph 2 and Article 10(1)(f).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		72(2).		***other consultations, particularly on the basis of police checks,***>>[90]
222	4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation.	4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted ***two*** years after their creation.	4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation.	4. The logs may be used only for the purpose referred to in paragraph 1 and shall be deleted ***two*** years after their creation. Subject to the outcome of the discussions on Art. 18(4).
223	5. Logs may be kept longer if they are required for monitoring procedures that are already under way.		5. Logs may be kept longer if they are required for monitoring procedures that are already under way.	5. Logs may be kept longer if they are required for monitoring procedures that are already under way.
224	6. The competent national authorities in charge of checking whether or not searches are lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of the N.SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to these logs for the purpose of fulfilling their duties.		6. The ~~competent~~ national **supervisory** authorities in charge of checking whether or not searches are lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of the N.SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to these logs for the purpose of fulfilling their duties.	6. The competent national authorities in charge of checking whether or not searches are lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of the N.SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to these logs for the purpose of fulfilling their duties.
225	7. Where Member States carry out automated scanned searches of	7. Where Member States' ***national law*** allows automated scanned searches of the number	7. Where Member States carry out automated scanned searches of	7.

[90] This text is not common to the one in the same Article of the Borders proposal.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	the number plates of motor vehicles, using Automatic Number Plate Recognition systems, Member States shall maintain a log of the search in accordance with national law. The content of this log shall be established by means of implementing measures in accordance with the examination procedure referred to in Article 72(2). Where a positive match is achieved against data stored in SIS, or a national or technical copy of SIS data, a full search shall be carried out in SIS in order to verify that a match has indeed been achieved. The provisions of paragraphs 1 to 6 of this Article shall apply to this full search.	plates of motor vehicles, ***and Member States carry out such searches*** using Automatic Number Plate Recognition systems, Member States shall maintain a log of the search. The ***Commission*** shall be ***empowered to adopt a delegated act*** in accordance with ***Article 71a establishing the rules regarding such logs.*** Where a positive match is achieved against data stored in SIS, or a national or technical copy of SIS data, a full search shall be carried out in SIS in order to verify that a match has indeed been achieved. The provisions of paragraphs 1 to 6 of this Article shall apply to this full search.	the number plates of motor vehicles, using Automatic Number Plate Recognition systems, Member States shall maintain a log of the search in accordance with national law. ~~The content of this log shall be established by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[91]~~. Where a positive match is achieved against data stored in SIS, or a national or technical copy of SIS data, a full search shall be carried out in SIS in order to verify that a match has indeed been achieved. The provisions of paragraphs 1 to 6 of this Article shall apply to this full search.~~	To be checked.
226			**8.**[92] **The Commission shall adopt implementing acts to establish the content of the log, referred to in paragraph 7. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**	To be checked.

[91] Text moved to new paragraph 8.
[92] Text moved from paragraph 7.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
227	*Article 13*	*Article 13*	*Article 13*	*Article 13*
228	*Self-monitoring*	*Self-monitoring*	*Self-monitoring*	*Self-monitoring*
229	Member States shall ensure that each authority entitled to access SIS data takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the national supervisory authority.	Member States shall ensure that each authority entitled to access SIS data takes the measures necessary to comply with this Regulation and cooperates with the national supervisory authority.	Member States shall ensure that each authority entitled to access SIS data takes the measures necessary to comply with this Regulation and cooperates, where necessary, with the national supervisory authority.	
230	*Article 14*	*Article 14*	*Article 14*	*Article 14*
231	*Staff training*	*Staff training*	*Staff training*	*Staff training*
232	Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training about data security, data protection rules and the procedures on data processing as set out in the SIRENE Manual. The staff shall be informed of any relevant criminal offences and penalties.	***1.*** Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training about data security, ***fundamental rights including*** data protection rules and the procedures on data processing as set out in the SIRENE Manual. The staff shall be informed of any relevant criminal offences and penalties ***laid down in accordance with Article 70a of this Regulation***.	Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training about data security, data protection rules and the procedures on data processing as set out in the SIRENE Manual. The staff shall be informed of any relevant criminal offences and penalties.	***1.*** Before being authorised to process data stored in SIS and periodically after access to SIS data has been granted, the staff of the authorities having a right to access SIS shall receive appropriate training about data-security, ***fundamental rights including*** data-protection rules and the procedures on data processing as set out in the SIRENE Manual. The staff shall be informed of any relevant criminal offences and penalties***, including those laid down in accordance with Article 70a of this Regulation***.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
233		***2. Member States shall have a national SIS training programme. This training programme shall include training for end-users as well as the staff of the SIRENE Bureaux.***		*2.* ***Member States shall have a national SIS training programme. This training programme shall include training for end-users as well as the staff of the SIRENE Bureaux.*** This training programme may be part of a generic training approach and programme at national level encompassing training in other relevant areas.
234		***3. Common training courses shall be organised at least once a year, to enhance cooperation between SIRENE Bureaux by allowing staff to meet colleagues from other SIRENE Bureaux, by allowing staff to meet colleagues from other SIRENE Bureaux, share information on national working methods and create a consistent and equivalent level of knowledge.***		***3. Common training courses shall be organised <u>at EU level</u> at least once a year to enhance cooperation between SIRENE Bureaux.***
235	**CHAPTER III**		**CHAPTER III**	**CHAPTER III**
236	**RESPONSIBILITIES OF THE AGENCY**		**RESPONSIBILITIES OF THE AGENCY**	**RESPONSIBILITIES OF THE AGENCY**
237	*Article 15*	*Article 15*	*Article 15*	*Article 15*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
238	*Operational management*	*Operational management*	*Operational management*	*Operational management*
239	1. The Agency shall be responsible for the operational management of Central SIS. The Agency shall, in cooperation with the Member States, ensure that at all times the best available technology, using a cost-benefit analysis, is used for Central SIS.		1. The Agency shall be responsible for the operational management of Central SIS. The Agency shall, in cooperation with the Member States, ensure that at all times the ~~best available~~ **most appropriate** technology, using a cost-benefit analysis, is used for Central SIS.	LIBE proposal: 1. The Agency shall be responsible for the operational management of Central SIS. The Agency shall ~~ensure~~, in cooperation with the Member States, ensure that at all times the best available technology, ***subject to*** ~~using~~ a cost-benefit analysis, is used for Central SIS.
240	2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure.		2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure.	[93] 2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure.
241	(a) supervision;		(a) supervision;	(a) supervision;
242	(b) security;		(b) security;	(b) security;
243	(c) the coordination of relations between the Member States and the provider;		(c) the coordination of relations between the Member States and the provider;	(c) the coordination of relations between the Member States and the provider;
244		***(ca) tasks relating to implementation of the budget;***		***(ca) tasks relating to implementation of the budget;***
245		***(cb) acquisition and renewal;***		***(cb) acquisition and renewal;***

[93] Further proceedings depend on the progress of the negotiations regarding the eu-LISA Regulation. Paragraph to be considered being in [].

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
246		***(cc) contractual matters.***		***(cc) contractual matters.***
247	3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:	***deleted***	3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:	Paragraph 3 could be deleted as a consequence of the additions to paragraph 2.
248	(a) tasks relating to implementation of the budget;		(a) tasks relating to implementation of the budget;	
249	(b) acquisition and renewal;		(b) acquisition and renewal;	
250	(c) contractual matters.		(c) contractual matters.	
251	4. The Agency shall be responsible for the following tasks relating to the SIRENE Bureaux and communication between the SIRENE Bureaux:		4. The Agency shall **also**[94] be responsible for the following tasks relating to the SIRENE Bureaux and communication between the SIRENE Bureaux:	4. The Agency shall also be responsible for the following tasks relating to the SIRENE Bureaux and communication between the SIRENE Bureaux:
252	(a) the coordination and management of testing;		(a) the coordination**,** ~~and~~ management **and support** of testing **activities**;	(a) the coordination**,** ~~and~~ management **and support** of testing **activities**;
253	(b) the maintenance and update of technical specifications for the exchange of supplementary information between SIRENE Bureaux and the Communication		(b) the maintenance and update of technical specifications for the exchange of supplementary information between SIRENE Bureaux and the Communication	(b) the maintenance and update of technical specifications for the exchange of supplementary information between SIRENE Bureaux and the Communication

[94] To align the texto with the similar provision in Borders proposal.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Infrastructure and managing the impact of technical changes where it affects both SIS and the exchange of supplementary information between SIRENE Bureaux.		Infrastructure and managing the impact of technical changes where it affects both SIS and the exchange of supplementary information between SIRENE Bureaux.	Infrastructure and managing the impact of technical changes where it affects both SIS and the exchange of supplementary information between SIRENE Bureaux.
254	5. The Agency shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS and shall provide regular reports to the Member States. The Agency shall provide a regular report to the Commission covering the issues encountered and the Member States concerned. This mechanism, procedures and the interpretation of data quality compliance shall be established by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	5. The Agency shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS and shall provide regular ***lists and*** reports to the Member States. The Agency shall provide a regular report to the ***European Parliament, the Council and the*** Commission covering the issues encountered and the Member States concerned. This mechanism, procedures and the interpretation of data quality compliance shall be established by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	5. The Agency shall develop and maintain a mechanism and procedures for carrying out quality checks on the data in CS-SIS and shall provide regular reports to the Member States. The Agency shall provide a regular report to the Commission covering the issues encountered and the Member States concerned. ~~This mechanism, procedures and the interpretation of data quality compliance shall be established by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[95]	LIBE maintains its position Commission services suggestion: issues on quality of data could be included in the technical report produced by eu-LISA COM suggestion is acceptable for the Council. LIBE does not agree with this suggestion but maintains its text (this text as in Parliament column was provisionally agreed in ETIAS)
255		***5a. The Agency shall also perform tasks related to providing training on the technical use of SIS and on measures to improve***		***5a. The Agency shall also perform tasks related to providing training on the technical use of***

[95] Text moved to new paragraph 7.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		the quality of SIS data.		***SIS and on measures to improve the quality of SIS data.***
256	6. Operational management of Central SIS shall consist of all the tasks necessary to keep Central SIS functioning 24 hours a day, seven days a week, in particular the maintenance work and technical developments necessary for the smooth running of the system. Those tasks also include testing activities ensuring that Central SIS and the national systems operate in accordance with the technical and functional requirements in accordance with Article 9 of this Regulation.		6. Operational management of Central SIS shall consist of all the tasks necessary to keep Central SIS functioning 24 hours a day, seven days a week **in accordance with this Regulation**, in particular the maintenance work and technical developments necessary for the smooth running of the system. Those tasks also include **the coordination, management and support of** testing activities **for Central SIS and the national systems,** ensuring that Central SIS and the national systems operate in accordance with the technical and functional requirements in accordance with Article 9 of this Regulation.	6. Operational management of Central SIS shall consist of all the tasks necessary to keep Central SIS functioning 24 hours a day, seven days a week ***in accordance with this Regulation***, in particular the maintenance work and technical developments necessary for the smooth running of the system. Those tasks also include **the coordination, management and support of** testing activities **for Central SIS and the national systems,** ensuring that Central SIS and the national systems operate in accordance with the technical and functional requirements in accordance with Article 9 of this Regulation.
257			**7.**[96] **The Commission shall adopt implementing acts to set out the technical requirements of the Communication Infrastructure referred to in paragraph 2, and to establish the mechanism and procedures for**	

[96] Text moved from paragraph 5.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			the quality checks on the data in CS-SIS referred to in paragraph 5 and for the interpretation of data quality compliance. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).	
258	*Article 16*	*Article 16*	*Article 16*	*Article 16*
259	*Security*	*Security*	*Security* ***- Agency***	*Security* ***- Agency***
260	1. The Agency shall adopt the necessary measures, including of a security plan, a business continuity plan and a disaster recovery plan for Central SIS and the Communication Infrastructure in order to:		1. The Agency shall adopt the necessary measures, including of a security plan, a business continuity plan and a disaster recovery plan for Central SIS and the Communication Infrastructure in order to:	1. The Agency shall adopt the necessary measures, including of a security plan, a business continuity plan and a disaster recovery plan for Central SIS and the Communication Infrastructure in order to:
261	(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;
262	(b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);	(b) deny unauthorised persons access to data-processing ***equipment and material and*** facilities used for processing personal data (***equipment,*** access control ***and facilities entry***	(b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control);	(see under Article 10)

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		control);		
263	(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);		(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);	(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
264	(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);		(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);	(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
265	(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);		(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);	(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);
266		***(ea) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry);***		(see under Article 10)
267	(f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation by		(f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation by	(f) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation by

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	means of individual and unique user identities and confidential access modes only (data access control);		means of individual and unique user ~~identities~~**identifiers** and confidential access modes only (data access control);	means of individual and unique user ~~identities~~**identifiers** and confidential access modes only (data access control);
268	(g) create profiles describing the functions and responsibilities for persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 64 without delay upon its request (personnel profiles);	(g) create profiles describing the functions and responsibilities for persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 64 ***immediately*** upon its request (personnel profiles);	(g) create profiles describing the functions and responsibilities for persons who are authorised to access the data or the data processing facilities and make these profiles available to the European Data Protection Supervisor referred to in Article 64 without delay upon its request (personnel profiles);	
269	(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);		(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);	(h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
270	(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom		(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom	(i) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when and by whom

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	the data were input (input control);		the data were input (input control);	the data were input (input control);
271	(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media in particular by means of appropriate encryption techniques (transport control);		(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media in particular by means of appropriate encryption techniques (transport control);	(j) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media in particular by means of appropriate encryption techniques (transport control);
272	(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).		(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).	(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).
273		***(ka) ensure that the system installed may, in case of interruption, be restored (recovery);***		(see under Article 10)
274		***(kb) ensure that SIS performs its functions correctly, that faults are reported (reliability) and that personal data stored in SIS cannot***		(see under Article 10)

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		be corrupted by means of the system malfunctioning (integrity);		
275		***(kc) ensure the security of its technical sites.***		As the system is hosted in the technical sites is important to stress the overall responsibility of the Agency for the security of its technical sites.
276	2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information through the Communication Infrastructure.		2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information through the Communication Infrastructure.	2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards security in respect of the processing and exchange of supplementary information through the Communication Infrastructure.
277	*Article 17*	*Article 17*	*Article 17*	*Article 17*
278	*Confidentiality – The Agency*	*Confidentiality – The Agency*	*Confidentiality – ~~The~~ Agency*	*Confidentiality – ~~The~~ Agency*
279	1. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in Article 11 of this Regulation to all its staff required to work with SIS data. This		1. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in Article 11 of this Regulation to all its staff required to work with SIS data. This	1. Without prejudice to Article 17 of the Staff Regulations of officials and the Conditions of Employment of other servants of the European Union, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality of comparable standards to those laid down in Article 11 of this Regulation to all its staff required to work with SIS data. This

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	obligation shall also apply after those persons leave office or employment or after the termination of their activities.		obligation shall also apply after those persons leave office or employment or after the termination of their activities.	obligation shall also apply after those persons leave office or employment or after the termination of their activities.
280	2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards confidentiality in respect of the exchange of supplementary information through the communication infrastructure.		2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards confidentiality in respect of the exchange of supplementary information through the **C**ommunication **I**nfrastructure.	2. The Agency shall take measures equivalent to those referred to in paragraph 1 as regards confidentiality in respect of the exchange of supplementary information through the **C**ommunication **I**nfrastructure.
281		***2a. Where the Agency cooperates with external contractors in any SIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.***		***2a. Where the Agency cooperates with external contractors in any SIS-related tasks, it shall closely monitor the activities of the contractor to ensure compliance with all provisions of this Regulation, including in particular security, confidentiality and data protection.*** The operational management of ~~[N.]~~***CS-***SIS [~~or of any technical copies~~] shall not be entrusted to private companies or private organisations.
282	*Article 18*	*Article 18*	*Article 18*	*Article 18*
283	*Keeping of logs at central level*	*Keeping of logs at central level*	*Keeping of logs at central level*	*Keeping of logs at central level*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
284	1. The Agency shall ensure that every access to and all exchanges of personal data within CS-SIS are logged for the purposes mentioned in Article 12(1).		1. The Agency shall ensure that every access to and all exchanges of personal data within CS-SIS are logged for the purposes mentioned in Article 12(1).	1. The Agency shall ensure that every access to and all exchanges of personal data within CS-SIS are logged for the purposes mentioned in Article 12(1).
285	2. The logs shall show, in particular, the history of the alerts, the date and time of the data transmitted, the type of data used to perform searches, the reference to the type of data transmitted and the name of the competent authority responsible for processing the data.	2. The logs shall show, in particular, the history of ***each alert***, the date and time of ***any data processing activity,*** the type of data used to perform ***a search***, the data ***processed*** and ***both*** the name of the competent authority ***and the person performing the search and*** processing the data.	2. The logs shall show, in particular, the history of the ~~alerts~~**alert**[97], the date and time of the data transmitted, the ~~type of~~ data used to perform searches, ~~the~~ **a** reference to the ~~type of~~ data transmitted and the ~~name~~**individual and unique user identifiers**[98] of the competent authority responsible for processing the data.	Commission services proposal of 12 Jan 2018: 2. The logs shall show, in particular, the history of ~~***each***~~ **the** alert, the date and time of ~~***any***~~ **the** data processing activity, the ~~type of~~ data used to perform a search, **a reference to** the data ***processed*** and ~~***both***~~ the ~~name~~ **individual and unique user identifiers** of the competent authority ~~and the person performing a search and~~ ***processing*** the data. LIBE to check.
286	3. If the search is carried out with dactylographic data or facial image in accordance with Articles 40, 41 and 42 the logs shall show, in particular, the type of data used to perform the search, a reference to the type data transmitted and the	3. ***By way of derogation to paragraph 2,*** if the search is carried out with dactylographic data or facial image in accordance with Articles 40, 41 and 42 the logs shall show the type ***of*** data ***processed instead of the actual***	3. If the search is carried out with dactylo~~graphic~~**scopic** data or facial image in accordance with Articles 40, 41 and 42 the logs shall show, in particular, the type of data used to perform the search, a reference to the type **of** data	Commission services proposal of 12 Jan 2018: ***3 By way of derogation from paragraph 2, if*** the search is carried out with ***dactyloscopic*** data or facial image in accordance with Article 22 the logs shall show the

[97] Singular, as in Article 12(2).
[98] Same wording as in Articles 10(1)(f) and 12(2) and (3).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	names of both the competent authority and the person responsible for processing the data.	***data.***	transmitted and the ~~names~~**individual and unique identifiers** of both the competent authority and the person responsible for processing the data.	type of data ***~~processed~~ used to perform the search instead of*** the ***actual*** data. The logs shall also contain a reference to the type of data ~~transmitted~~ ***processed*** and the ***individual and unique user identifiers*** of ~~both~~ the competent authority ~~and the person responsible for~~ processing the data. LIBE to check.
287		***3a. Rules and formats for logs shall be laid down by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).***		Presidency maintains its position. As part of an overall compromise, could be withdrawn.
288	4. The logs may only be used for the purposes mentioned in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation. The logs which include the history of alerts shall be erased after one to three years after deletion of the alerts.	4. The logs may only be used for the purposes mentioned in paragraph 1 and shall be deleted ***two years*** after their creation. The logs which include the history of alerts shall be erased after ***two*** years after deletion of the alerts.	4. The logs may only be used for the purposes mentioned in paragraph 1 and shall be deleted at the earliest one year, and at the latest three years, after their creation. The logs which include the history of alerts shall be erased after one to three years after deletion of the alerts.	After confirmation by eu-LISA, the Presidency would propose a compromise draft.
289	5. Logs may be kept longer if they are required for monitoring		5. Logs may be kept longer if they are required for monitoring	5. Logs may be kept longer if they are required for monitoring

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	procedures that are already underway.		procedures that are already underway.	procedures that are already underway.
290	6. The competent authorities in charge of checking whether or not a search is lawful, monitoring the lawfulness of data processing, self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security, shall have access, within the limits of their competence and at their request, to those logs for the purpose of fulfilling their tasks.		6. The ~~competent authorities in charge of checking whether or not a search is lawful, monitoring the lawfulness of data processing, self monitoring and ensuring the proper functioning of CS-SIS, data integrity and security,~~**European Data Protection Supervisor** shall have access, within the limits of ~~their~~**its** competence and at ~~their~~**its** request, to those logs for the purpose of fulfilling ~~their~~**its** tasks.	6. ~~The competent authorities in charge of checking whether or not a search is lawful, monitoring the lawfulness of data processing,~~ For the purposes of self-monitoring and ensuring the proper functioning of CS-SIS, data integrity and security, the Agency shall have access, within the limits of its competence ~~and at their request~~, to those logs. ***The European Data Protection Supervisor*** shall have access, within the limits of its competence and at its request, to those logs for the purpose of fulfilling its tasks.
291	**CHAPTER IV**		**CHAPTER IV**	**CHAPTER IV**
292	**INFORMATION TO THE PUBLIC**		**INFORMATION TO THE PUBLIC**	**INFORMATION TO THE PUBLIC**
293	*Article 19*	*Article 19*	*Article 19*	*Article 19*
294	*SIS information campaigns*	*SIS information campaigns*	*SIS information campaigns*	*SIS information campaigns*
295	The Commission, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, shall	1. ***At the start of the application of this Regulation,*** The Commission, in cooperation with the national supervisory authorities and the European Data	The Commission, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, shall	Latest proposal for compromise: **At the start of application of this Regulation, the** Commission, in cooperation with the national

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	regularly carry out campaigns informing the public about the objectives of SIS, the data stored, the authorities having access to SIS and the rights of data subjects. Member States shall, in cooperation with their national supervisory authorities, devise and implement the necessary policies to inform their citizens about SIS generally.	Protection Supervisor, shall carry out a campaign informing ***EU citizens and third-country nationals*** about the objectives of SIS, the data stored, the authorities having access to SIS and the rights of data subjects. ***The Commission, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, shall repeat such campaigns regularly at least once per year***. Member States shall, in cooperation with their national supervisory authorities, devise and implement the necessary policies to inform their citizens ***and residents*** about SIS generally. ***Member States shall ensure that sufficient funding is made available for such information policies.***	regularly carry out campaigns informing the public about the objectives of SIS, the data stored, the authorities having access to SIS and the rights of data subjects. Member States shall, in cooperation with their national supervisory authorities, devise and implement the necessary policies to inform their citizens about SIS generally.	supervisory authorities and the European Data Protection Supervisor, shall carry out **a campaign** informing **the public** ~~**Union citizens and third country nationals**~~ about the objectives of SIS, the data stored, the authorities having access to SIS and the rights of data subjects. **The Commission, in cooperation with the national supervisory authorities and the European Data Protection Supervisor, shall repeat such campaigns regularly** ~~**at least once per year.**~~ **The Commission shall maintain a website available to the public on all relevant information concerning SIS.** Member States shall, in cooperation with their national supervisory authorities, devise and implement the necessary policies to inform their citizens **and residents** about SIS generally. ~~***Member States shall ensure that sufficient funding is made available for such information policies.***~~
296	**CHAPTER V**	**CHAPTER V**	**CHAPTER V**	
297	**CATEGORIES OF DATA AND FLAGGING**	**CATEGORIES OF DATA AND FLAGGING**	**CATEGORIES OF DATA AND FLAGGING**	
298	*Article 20*	*Article 20*	*Article 20*	*Article 20*
299	*Categories of data*	*Categories of data*	*Categories of data*	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
300	1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, SIS shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Articles 26, 32, 34, 36 and 38.	1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, SIS shall contain only those categories of data which are supplied by each Member ***State***, as required for the purposes laid down in Articles 26, 32, 34, 36 and 38.	1. Without prejudice to Article 8(1) or the provisions of this Regulation providing for the storage of additional data, SIS shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Articles 26, 32, 34, 36**,**~~and~~ 38 **and 40**.	
301	2. The categories of data shall be as follows:		2. The categories of data shall be as follows:	
302	(a) information on persons in relation to whom an alert has been issued;		(a) information on persons in relation to whom an alert has been issued;	
303	(b) information on objects referred to in Articles 32, 36 and 38.		(b) information on objects referred to in Articles **26,** 32, **34,** 36 and 38.	
304	3. The information on persons in relation to whom an alert has been issued shall only contain the following data:	3. The information on persons in relation to whom an alert has been issued ***for the purpose of police and judicial cooperation*** shall only contain the following data:	3. **Any alert in SIS which includes**~~The~~ information on persons ~~in relation to whom an alert has been issued~~ shall only contain the following data:	
305	(a) surname(s)		(a) surname~~(s)~~**;**	(a) surname~~(s)~~;
306	(b) forename(s),		(b) forename~~(s),~~**;**	(b) forename~~(s)~~;

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
307	(c) name(s) at birth		(c) name~~(s)~~ at birth**:**	(c) name~~(s)~~ at birth;
308	(d) previously used names and aliases;		(d) previously used names and aliases;	(d) previously used names and aliases;
309	(e) any specific, objective, physical characteristics not subject to change;	(e) any specific, objective, physical characteristics not subject to change***, not linked to special categories of personal data defined in Article 9 of Regulation (EU) 2016/679, such as ethnicity, religion, disability, gender or sexual orientation***;	(e) any specific, objective, physical characteristics not subject to change;	
310	(f) place of birth		(f) place of birth**:**	(f) place of birth;
311	(g) date of birth;		(g) date of birth;	(g) date of birth;
312	(h) sex;	(h) ***gender***;	(h) ~~sex~~**gender**;	(h) ***gender***;
313	(i) nationality/nationalities;		(i) nationality/nationalities;	(i) nationality / nationalities;
314	(j) whether the person concerned is armed, violent, has escaped or is involved in an activity as referred to in Articles 1, 2 , 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism;	(j) whether the person concerned is armed, violent, has escaped or is involved in an activity as referred to in ***Articles 3 to 12 and 14 of Directive (EU) 2017/541***;	(j) whether the person concerned: **i.** is armed**;** ~~,~~ **ii.** **is** violent ~~,~~**;** **iii.** has **absconded or** escaped**;** **iv.** **poses a risk of suicide;** **v.** **poses a threat to public health;** or	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			vi. is involved in a **terrorism-related** activity~~as referred to in Articles 1, 2 , 3 and 4 of Council Framework Decision 2002/475/JHA on combating terrorism~~;	
315	(k) reason for the alert;		(k) reason for the alert;	(k) reason for the alert;
316	(l) authority issuing the alert;		(l) authority issuing the alert;	(l) authority issuing the alert;
317	(m) a reference to the decision giving rise to the alert;		(m) a reference to the decision giving rise to the alert;	(m) a reference to the decision giving rise to the alert;
318	(n) action to be taken;		(n) action to be taken;	(n) action to be taken;
319	(o) link(s) to other alerts issued in SIS pursuant to Article 53;		(o) link(s) to other alerts issued in SIS pursuant to Article ~~53~~**60**;	(o) link(s) to other alerts issued in SIS pursuant to Article ~~53~~**60**;
320	(p) the type of offence for which the alert was issued;		(p) the type of offence for which the alert was issued;	(p) the type of offence for which the alert was issued;
321	(q) the person's registration number in a national register		(q) the person's registration number in a national register**;**	(q) the person's registration number in a national register**;**
322	(r) a categorisation of the type of missing person case (only for alerts referred to in Article 32);		(r) a categorisation of the type of missing person case (only for alerts referred to in Article 32);	(r) a categorisation of the type of missing person case (only for alerts referred to in Article 32);

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
323	(s) the category of the person's identification document;		(s) the category of the person's identification document**s**;	
324	(t) the country of issue of the person's identification document;		(t) the country of issue of the person's identification document**s**;	
325	(u) the number(s) of the person's identification document;		(u) the number(s) of the person's identification document**s**;	
326	(v) the date of issue of the person's identification document;		(v) the date of issue of the person's identification document**s**;	
327	(w) photographs and facial images;		(w) photographs and facial images;	(w) photographs and facial images;
328	(x) relevant DNA profiles subject to Article 22(1)(b) of this Regulation;	(x) ***where permitted, in accordance with*** Article 22(1)(b) ***and Article 32(2)(a)***, relevant DNA profiles;	(x) relevant DNA profiles subject to Article 22(1)(b) of this Regulation;	
329	(y) dactylographic data;	(y) ***dactyloscopic*** data;	(y) dactylo~~graphic~~**scopic** data;	(y) dactylo~~graphic~~**scopic** data;
330	(z) a colour copy of the identification document.		(z) a ~~colour~~ copy**, whenever possible in colour,** of the identification document**s**.	
331		***(za) data referred to in points (a) to (d), (f) to (g) and (i), from a valid identification document(s) carried by the person other than the document referred to in points***		

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		(s) to (v), insofar as such data is not available in the latter document.		
332		***Technical rules shall be similar for searches in CS-SIS, in national copies and in technical copies, as referred to in Article 53. They shall be based upon common standards laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).***		
333	4. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraphs 2 and 3 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).		4. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraphs 2 and 3 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	4. The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraphs 2 and 3 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).
334	5. The technical rules necessary for searching data referred to in paragraph 3 shall be laid down and developed in accordance with the examination procedure referred to in Article 72(2). These technical rules	***deleted***	5. ~~The technical rules necessary for searching data referred to in paragraph 3 shall be laid down and developed in accordance with the examination procedure referred to in~~	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	shall be similar for searches in CS-SIS, in national copies and in technical copies, as referred to in Article 53(2) and they shall be based upon common standards laid down developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).		~~Article 72(2).~~[99] These technical rules shall be similar for searches in CS-SIS, in national **or shared** copies and in technical copies, as referred to in Article 53(2) and they shall be based upon common standards laid down **and** developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	
335	*Article 21*	*Article 21*	*Article 21*	
336	*Proportionality*	*Proportionality*	*Proportionality*	
337	1. Before issuing an alert and when extending the validity period of an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant the entry of an alert in SIS.		1. Before issuing an alert and when extending the validity period of an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant the ~~entry~~**existence** of an alert in SIS.	
338	2. Where a person or an object is sought by a Member State in relation to an offence that falls under Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism, the Member State shall,	2. Where a person or an object is sought by a Member State in relation to an offence that falls under Articles ***3*** to ***12 and 14 of the Directive (EU) 2017/541,*** the Member State shall, in all circumstances, create the	2. Where a person or an object is sought by a Member State in relation to an offence that falls under Articles ~~1~~**3** to **1**4 of **Directive 2017/541 or is equivalent to those offences** ~~of Council Framework Decision~~	

[99] Redundant with paragraph 4.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	in all circumstances, create the corresponding alert under either Article 34, 36 or 38 as appropriate.	corresponding alert under either Article 34, 36 or 38 as appropriate.	~~2002/475/JHA on combating terrorism~~, the Member State shall~~,in all circumstances,~~ create a~~the~~ corresponding alert,~~under either Article 34, 36 or 38 as appropriate~~. **Exceptionally, Member States may refrain from creating the alert when it is likely to obstruct official or legal inquiries, investigations or procedures related to public or national security**.	
339	*Article 22*	*Article 22*	*Article 22*[100]	*Agreement to move it to Article 41A*
340	*Specific rules for entering photographs, facial images, dactylographic data and DNA profiles*	*Specific rules for entering photographs, facial images,* ***dactyloscopic*** *data and DNA profiles*	~~*Specific rules for entering photographs, facial images, dactyloscopic data and DNA profiles*~~	
341		***-1. The Commission shall be empowered to adopt delegated acts in accordance with Article 71 a concerning the requirements to be fulfilled for the entering of biometric identifiers, including DNA profiles, into SIS in accordance with this Regulation. Those requirements shall include the number of fingerprints to be***		See Article 41A

[100] Article moved to new Chapter XIa, as Article 41A.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		inserted, the method of capturing them and the minimum quality standard to be fulfilled by all biometric identifiers.		
342	1. The entering into SIS of data referred to in Article 20(3)(w), (x) and (y) shall be subject to the following provisions:		~~1. The entering into SIS of data referred to in Article 20(3)(w), (x) and (y) shall be subject to the following provisions:~~	
343	(a) Photographs, facial images, dactylographic data and DNA profiles shall only be entered following a quality check to ascertain the fulfilment of a minimum data quality standard.	(a) Photographs, facial images ***and dactyloscopic*** data shall only be entered following a quality check to ascertain the fulfilment of a minimum data quality standard.	~~(a) Photographs, facial images, dactylographic data and DNA profiles shall only be entered following a quality check to ascertain the fulfilment of a minimum data quality standard.~~	
344	(b) A DNA profile may only be added to alerts provided for in Article 32(2)(a) and (c) and only where photographs, facial images or dactylographic data suitable for identification are not available. The DNA profiles of persons who are direct ascendants, descendants or siblings of the alert subject may be added to the alert provided that those persons concerned gives explicit	(b) A DNA profile may only be added to alerts ***in the situations*** provided for in ***Article 32***(2)(a) ***only following a quality check to ascertain the profile fulfils a minimum data quality standard*** and only where photographs, facial images or ***dactyloscopic*** data suitable for identification are not available. The DNA profiles of persons who are direct ascendants, descendants or siblings of the alert subject may be added to the alert provided that those persons concerned gives explicit consent.	~~(b) A DNA profile may only be added to alerts provided for in Article 32(2)(a) and (c) and only where photographs, facial images or dactylographic data suitable for identification are not available. The DNA profiles of persons who are direct ascendants, descendants or siblings of the alert subject may be added to the alert provided that those persons concerned gives explicit~~	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	consent. The racial origin of the person shall not be included in the DNA profile.	***Where a DNA profile is added to an alert, that profile shall contain the minimum information strictly necessary for the identification of the missing person and, in all event, shall always exclude the racial origin and health information about that person***.	~~consent. The racial origin of the person shall not be included in the DNA profile.~~	
345	2. Quality standards shall be established for the storage of the data referred to under paragraph 1(a) of this Article and Article 40. The specification of these standards shall be laid down by means of implementing measures and updated in accordance with the examination procedure referred to in Article 72(2).	2 Quality standards shall be established for the storage of the data referred to under paragraph 1(a) ***and (b)*** of this Article and Article 40. The specification of these standards shall be laid down by means of implementing measures and updated in accordance with the examination procedure referred to in Article 72(2).	~~2. Quality standards shall be established for the storage of the data referred to under paragraph 1(a) of this Article and Article 40. The specification of these standards shall be laid down by means of implementing measures and updated in accordance with the examination procedure referred to in Article 72(2).~~	
346	*Article 23*	*Article 23*	*Article 23*	*Article 23*
347	*Requirement for an alert to be entered*	*Requirement for an alert to be entered*	*Requirement for an alert to be entered*	*Requirement for an alert to be entered*
348	1. An alert on a person may not be entered without the data referred to in Article 20(3)(a), (g), (k), (m), (n) as well as, where applicable, (p), except for in the situations referred to in Article 40.	1. An alert on a person may not be entered without the data referred to in Article 20(3)(a), ***(b),*** (g), ***(h), (i),*** (k), (m), (n) as well as, where applicable, (p), except for in the situations referred to in Article 40.	1. ~~An alert on a person may not be entered without the data referred to in Article 20(3)(a), (g), (k), (m), (n) as well as, where applicable, (p), except for in the situations referred to in Article~~	*To be seen in conjuction with the discussion in Article 4, last subpara. of the Returns text*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			~~40.~~[101] **All data listed in Article 20(3) shall be entered, where available.**[102]	
349	2. Where available, all other data listed in Article 20(3) shall also be entered.	2. ***Without prejudice to Article 22,*** where available, ***and provided that the conditions for entering the data have been met, the*** other data listed in Article 20(3) shall also be entered.	2. ~~Where available, all other data listed in Article 20(3) shall also be entered.~~[103] An alert on a person may not be entered without the data referred to in Article 20(3)(a), (g), (k), ~~(m),~~ (n) ~~as well as, where applicable,~~ ~~(p),~~ except for in the situations referred to in Article 40.[104]	*To be seen in conjuction with the discussion in Article 4 last subparagraph of the Returns text*
350		***Article 23a***		***Article 23a***
351		***Compatibility of alerts***		***Compatibility of alerts***
352		***1. Before entering a new alert, a Member State shall check whether the person is already the subject of an alert in SIS.***		Commission services adjustments of 9 January indicated in yellow: ***1. Before ~~entering a new~~ issuing an alert, ~~a~~ the Member State shall check whether the person or the object is already ~~the~~ subject of an alert in SIS. To check whether the person ~~appears in SIS under another identity~~ is already subject of an alert~~,~~ a ~~fingerprint~~ check with dactyloscopic data shall also be***

[101] Partially moved to paragraph 2.
[102] Partially moved from paragraph 2.
[103] Partially moved to paragraph 1.
[104] Partially moved from paragraph 1.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				carried out before a new alert is issued, if fingerprints are available. Acceptable for the Council. LIBE proposal: Modify last part to say: . ..”if ~~***fingerprints***~~ those data are available” COM will provide text to include provisions of point 2.2.3 of the SIRENE Manual (2018-03-26) Council’s compromise 03.04.2018 ***1. Before ~~entering a new~~ issuing an alert, ~~a~~ the Member State shall check whether the person or the object is already ~~the~~ subject of an alert in SIS. To check whether the person ~~appears in SIS under another identity~~ is already subject of an alert~~,~~ a ~~fingerprint~~ check with dactyloscopic data shall also be carried out before a new alert is issued, if ~~fingerprints~~ such data is available.***
353		***2. Only one alert per person or per object per Member State may be entered in SIS. However, where necessary, new alerts may be entered on the same person by***		Commission services adjustments of 9 January indicated in yellow: ***2. Only one alert per person ~~or~~ per object per Member State may be***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		other Member States, provided that they are compatible. The compatibility shall be ensured in accordance with paragraph 3.		***entered in SIS ~~II~~. However, where necessary, new alerts may be entered on the same person or on object by other Member States, ~~provided that they are compatible. The compatibility shall be ensured~~ in accordance with paragraph 3.*** Acceptable for the Council.
354		***3. Rules on the compatibility of alerts shall be laid down in the SIRENE Manual referred to in Article 8(4). Where a person is already the subject of an alert in SIS, a Member State wishing to enter a new alert shall check that there is no incompatibility between the alerts. If there is no incompatibility, the Member State may enter the new alert. If the alerts are incompatible, the SIRENE Bureaux concerned shall consult with each other by exchanging supplementary information in order to reach an agreement in line with the order of priority referred to in the SIRENE Manual. Departures from that order of priority may be made after consultation between the Member States if essential national interests are at stake.***		Commission services proposal of 9 January modified in 12 March 2018: ***3. Rules on the compatibility of alerts shall be laid down in the SIRENE Manual referred to in Article 8(4). Where a person or an object is already the subject of an alert in SIS, a Member State wishing to enter a new alert shall check that there is no incompatibility between the alerts. If there is no incompatibility, the Member State may enter the new alert. If the alerts are incompatible, the SIRENE Bureaux concerned shall consult with each other by exchanging supplementary information in order to reach an agreement ~~in line with the order of priority referred to in the SIRENE Manual~~. Departures from ~~that order of priority~~ compatibility rules may be made after consultation between the Member States if essential national interests are at stake.***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
355				COM services proposal (in conjunction with the deletion of art. 39(6) and 2.2.1. of SIRENE Manual): 4. In case of multiple hits on the same person or object the executing Member State shall observe the priority rules of alerts as laid down in the SIRENE Manual. In case a person is subject to several alerts issued by different Member States alerts for arrest issued pursuant to Article 26 shall be executed as a priority subject to Article 25.
356	*Article 24*	*Article 24*	*Article 24*	*Article 24*
357	*General provisions on flagging*	***Flagging***	*General provisions on flagging*	*General provisions on flagging*
358	1. Where a Member State considers that to give effect to an alert entered in accordance with Articles 26, 32 and 36 is incompatible with its national law, its international obligations or essential national interests, it may subsequently require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. The flag shall be added	1. Where a Member State considers that to give effect to an alert entered in accordance with Articles 26, 32**,** 36 ***and 40*** is incompatible with its national law, its international obligations or essential national interests, it may subsequently require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. The flag shall be added by the SIRENE Bureau of the	1. Where a Member State considers that to give effect to an alert entered in accordance with Articles 26, 32 **or**~~and~~ 36 is incompatible with its national law, its international obligations or essential national interests, it may subsequently require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. The flag shall be added	1. Where a Member State considers that to give effect to an alert entered in accordance with Articles 26, 32 **or** 36 is incompatible with its national law, its international obligations or essential national interests, it may subsequently require that a flag be added to the alert to the effect that the action to be taken on the basis of the alert will not be taken in its territory. The flag shall be added

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	by the SIRENE Bureau of the issuing Member State.	issuing Member State.	by the SIRENE Bureau of the issuing Member State.	by the SIRENE Bureau of the issuing Member State.
359	2. In order to enable Member States to require that a flag be added to an alert issued in accordance with Article 26, all Member States shall be notified automatically about any new alert of that category by the exchange of supplementary information.		2. In order to enable Member States to require that a flag be added to an alert issued in accordance with Article 26, all Member States shall be notified automatically about any new alert of that category by the exchange of supplementary information.	2. In order to enable Member States to require that a flag be added to an alert issued in accordance with Article 26, all Member States shall be notified automatically about any new alert of that category by the exchange of supplementary information.
360	3. If in particularly urgent and serious cases, an issuing Member State requests the execution of the action, the Member State executing the alert shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.		3. If in particularly urgent and serious cases, an issuing Member State requests the execution of the action, the Member State executing the alert shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.	3. If in particularly urgent and serious cases, an issuing Member State requests the execution of the action, the Member State executing the alert shall examine whether it is able to allow the flag added at its behest to be withdrawn. If the executing Member State is able to do so, it shall take the necessary steps to ensure that the action to be taken can be carried out immediately.
361	*Article 25*	*Article 25*	*Article 25*	*Article 25*
362	*Flagging related to alerts for arrest for surrender purposes*	*Flagging related to alerts for arrest for surrender purposes*	*Flagging related to alerts for arrest for surrender purposes*	*Flagging related to alerts for arrest for surrender purposes*
363	1. Where Framework Decision 2002/584/JHA applies, a flag preventing arrest shall only be		1. Where Framework Decision 2002/584/JHA applies, a flag preventing arrest shall ~~only~~ be	1. Where Framework Decision 2002/584/JHA applies, a flag preventing arrest shall ~~only~~ be

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	added to an alert for arrest for surrender purposes where the competent judicial authority under national law for the execution of a European Arrest Warrant has refused its execution on the basis of a ground for non-execution and where the addition of the flag has been required.		added to an alert for arrest for surrender purposes where the competent judicial authority under national law for the execution of a European Arrest Warrant has refused its execution on the basis of a ground for non-execution and where the addition of the flag has been required.	added to an alert for arrest for surrender purposes where the competent judicial authority under national law for the execution of a European Arrest Warrant has refused its execution on the basis of a ground for non-execution and where the addition of the flag has been required.
364			**A Member State may also require that a flag be added to the alert if its competent judicial authority releases the subject of the alert during the surrender process.**	**A Member State may also require that a flag be added to the alert if its competent judicial authority releases the subject of the alert during the surrender process.**
365	2. However, at the behest of a competent judicial authority under national law, either on the basis of a general instruction or in a specific case, a flag may also be required to be added to an alert for arrest for surrender purposes if it is obvious that the execution of the European Arrest Warrant will have to be refused.		2. However, at the behest of a competent judicial authority under national law, either on the basis of a general instruction or in a specific case, a flag may also be required to be added to an alert for arrest for surrender purposes if it is obvious that the execution of the European Arrest Warrant will have to be refused.	2. However, at the behest of a competent judicial authority under national law, either on the basis of a general instruction or in a specific case, a flag may also be required to be added to an alert for arrest for surrender purposes if it is obvious that the execution of the European Arrest Warrant will have to be refused.
366	**CHAPTER VI**		**CHAPTER VI**	**CHAPTER VI**
367	**ALERTS IN RESPECT OF PERSONS WANTED FOR**		**ALERTS IN RESPECT OF PERSONS WANTED FOR**	**ALERTS IN RESPECT OF PERSONS WANTED FOR**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	ARREST FOR SURRENDER OR EXTRADITION PURPOSES		**ARREST FOR SURRENDER OR EXTRADITION PURPOSES**	**ARREST FOR SURRENDER OR EXTRADITION PURPOSES**
368	*Article 26*		*Article 26*	*Article 26*
369	*Objectives and conditions for issuing alerts*		*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*
370	1. Data on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes shall be entered at the request of the judicial authority of the issuing Member State.		1. Data on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes shall be entered at the request of the judicial authority of the issuing Member State.	1. Data on persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes shall be entered at the request of the judicial authority of the issuing Member State.
371	2. Data on persons wanted for arrest for surrender purposes shall also be entered on the basis of arrest warrants issued in accordance with Agreements concluded between the Union and third countries on the basis of Article 37 of the Treaty on the European Union for the purpose of surrender of persons on the basis of an arrest warrant, which provide for the transmission of such an arrest warrant via the SIS.		2. Data on persons wanted for arrest for surrender purposes shall also be entered on the basis of arrest warrants issued in accordance with Agreements concluded between the Union and third countries on the basis of Article 37 of the Treaty on the European Union for the purpose of surrender of persons on the basis of an arrest warrant, which provide for the transmission of such an arrest warrant via the SIS.	2. Data on persons wanted for arrest for surrender purposes shall also be entered on the basis of arrest warrants issued in accordance with Agreements concluded between the Union and third countries on the basis of Article 37 of the Treaty on the European Union ***or Article 216 of the Treaty on the Functioning of*** the European Union for the purpose of surrender of persons on the basis of an arrest warrant, which provide for the transmission of such an arrest warrant via the SIS.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
372	3. Any reference in this Regulation to provisions of the Framework Decision 2002/584/JHA shall be construed as including the corresponding provisions of Agreements concluded between the European Union and third countries on the basis of Article 37 the Treaty on the European Union for the purpose of surrender of persons on the basis of an arrest warrant which provide for the transmission of such an arrest warrant via SIS.	3. Any reference in this Regulation to provisions of the Framework Decision 2002/584/JHA shall be construed as including the corresponding provisions of Agreements concluded between the European Union and third countries on the basis of Article ***216 of*** the Treaty on ***the functioning of*** the European Union for the purpose of surrender of persons on the basis of an arrest warrant which provide for the transmission of such an arrest warrant via SIS.	3. Any reference in this Regulation to provisions of the Framework Decision 2002/584/JHA shall be construed as including the corresponding provisions of Agreements concluded between the European Union and third countries on the basis of Article 37 the Treaty on the European Union for the purpose of surrender of persons on the basis of an arrest warrant which provide for the transmission of such an arrest warrant via SIS.	3. Any reference in this Regulation to provisions of the Framework Decision 2002/584/JHA shall be construed as including the corresponding provisions of Agreements concluded between the European Union and third countries on the basis of Article 37 ***of*** the Treaty on the European Union ***or Article 216 of*** the Treaty on ***the Functioning of*** the European Union for the purpose of surrender of persons on the basis of an arrest warrant which provide for the transmission of such an arrest warrant via SIS.
373	4. The issuing Member State may, in the case of an ongoing search operation and following the authorisation of the relevant judicial authority of the issuing Member State, temporarily make an existing alert for arrest issued under Article 26 of this Regulation unavailable for searching to the effect that the alert shall not be searchable by the end-user and will only be accessible to the SIRENE Bureaux. This functionality shall be used for a period not exceeding 48 hours. If operationally	4. The issuing Member State may, in the case of an ongoing search operation and following the authorisation of the relevant judicial authority of the issuing Member State, temporarily make an existing alert for arrest issued under ***this*** Article unavailable for searching to the effect that the alert shall not be searchable by the end-user and will only be accessible to the SIRENE Bureaux. This functionality shall be used for a period not exceeding 48 hours. If operationally necessary, however,	4. ~~The issuing Member State may, i~~**I**n the case of an ongoing ~~search~~ operation**, the issuing Member State may temporarily make an existing alert for arrest issued under Article 26 unavailable for searching to the effect that the alert shall not be searchable by the end-user in the Member States involved in the operation and will only be accessible to the SIRENE Bureaux, where the following conditions are met:**	**4. I**n the case of an ongoing ~~search~~ operation**, the issuing Member State may temporarily make an existing alert for arrest issued under *this* Article unavailable for searching by the end-users in the Member States involved in the operation. In that case *the alert* shall only be accessible to the SIRENE Bureaux. Member States shall only do so if :** **(a) the purpose of the operation cannot be**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	necessary, however, it may be extended by further periods of 48 hours. Member States shall keep statistics about the number of alerts where this functionality has been used.	it may be extended by further periods of 48 hours. Member States shall keep statistics about the number of alerts where this functionality has been used.	**(a)** ~~where~~ **the purpose of the operation cannot be achieved by other measures;** **(b)** ~~and following the~~ **a prior** authorisation ~~of~~ **has been granted by** the relevant judicial authority of the issuing Member State**; and** **(c) all Member States involved in the operation have been informed through the exchange of supplementary information.** ~~, temporarily make an existing alert for arrest issued under Article 26 of this Regulation unavailable for searching to the effect that the alert shall not be searchable by the end-user and will only be accessible to the SIRENE Bureaux.~~ Th~~e~~**e** functionality **provided for in the first subparagraph** shall **only** be used for a period not exceeding 48 hours ~~with the authorisation of the relevant judicial authority of the issuing Member State after informing all Member States involved in the operation, through the exchange of supplementary information~~. **However, i**f operationally necessary, ~~however,~~ it	**achieved by other measures;** **(b)** ~~a~~ **a prior** authorisation ~~of~~ **has been granted by** the relevant judicial authority of the issuing Member State**; and** **(c) all Member States involved in the operation have been informed through the exchange of supplementary information.** The functionality **provided for in the first subparagraph** shall **only** be used for a period not exceeding 48 hours. **However, i**f operationally necessary, it may be extended by further periods of 48 hours. Member States shall keep statistics about the number of alerts where this functionality has been used.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			may be extended by further periods of 48 hours. Member States shall keep statistics about the number of alerts where this functionality has been used.	
374			**5. Where there is a clear indication that the object referred to in Article 38 (2)(a), (b), (c), (e), (g), (h) and (k) are connected with a person who is the subject of an alert pursuant to paragraph 1 and 2, alerts on those objects may be issued in order to locate the person. In those cases the alert on the person and the alert on the object shall be linked in accordance with Article 60.**	*Informal outcome of technical discussion to be confirmed by trilogue* **5. Where there is a clear indication that the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), [(i)] and (k) are connected with a person who is the subject of an alert pursuant to paragraph 1 and 2 of this Article, alerts on those objects may be issued in order to locate the person. In those cases the alert on the person and the alert on the object shall be linked in accordance with Article 60.**
375			**6. The Commission shall adopt implementing acts to lay down and develop rules necessary for entering, updating, deleting and searching the data referred to in paragraph 5. Those implementing acts shall be adopted in accordance with the**	**6. The Commission shall adopt implementing acts to lay down and develop rules necessary for entering, updating, deleting and searching the data referred to in paragraph 5. Those implementing acts shall be adopted in accordance with the**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			examination procedure referred to in Article 72(2).	**examination procedure referred to in Article 72(2).**
376	*Article 27*	*Article 27*	*Article 27*	*Article 27*
377	*Additional data on persons wanted for arrest for surrender purposes*	*Additional data on persons wanted for arrest for surrender purposes*	*Additional data on persons wanted for arrest for surrender purposes*	*Additional data on persons wanted for arrest for surrender purposes*
378	1. Where a person is wanted for arrest for surrender purposes on the basis of a European Arrest Warrant the issuing Member State shall enter in SIS a copy of the original of the European Arrest Warrant.		1. Where a person is wanted for arrest for surrender purposes on the basis of a European Arrest Warrant the issuing Member State shall enter in SIS a copy of the original of the European Arrest Warrant.	1. Where a person is wanted for arrest for surrender purposes on the basis of a European Arrest Warrant the issuing Member State shall enter in SIS a copy of the original of the European Arrest Warrant. COM Services proposal related to 3.1. of SIRENE Manual: ***A Member State shall be able to enter the copy of one or more European Arrest Warrant to an alert for arrest.***
379	2. The issuing Member State may enter a copy of a translation of the European Arrest Warrant in one or more other official languages of the institutions of the European Union.		2. The issuing Member State may enter a copy of a translation of the European Arrest Warrant in one or more other official languages of the institutions of the European Union.	2. The issuing Member State may enter a copy of a translation of the European Arrest Warrant in one or more other official languages of the institutions of the European Union.
380	*Article 28*		*Article 28*	*Article 28*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
381	*Supplementary information on persons wanted for arrest for surrender purposes*		*Supplementary information on persons wanted for arrest for surrender purposes*	*Supplementary information on persons wanted for arrest for surrender purposes*
382	The Member State which entered the alert in SIS for arrest for surrender purposes shall communicate the information referred to in Article 8(1) of Framework Decision 2002/584/JHA to the other Member States through the exchange of supplementary information.		The Member State which entered the alert in SIS for arrest for surrender purposes shall communicate the information referred to in Article 8(1) of Framework Decision 2002/584/JHA to the other Member States through the exchange of supplementary information.	The Member State which entered the alert in SIS for arrest for surrender purposes shall communicate the information referred to in Article 8(1) of Framework Decision 2002/584/JHA to the other Member States through the exchange of supplementary information.
383	*Article 29*		*Article 29*	*Article 29*
384	*Supplementary information on persons wanted for arrest for extradition purposes*		*Supplementary information on persons wanted for arrest for extradition purposes*	*Supplementary information on persons wanted for arrest for extradition purposes*
385	1. The Member State which entered the alert into SIS for extradition purposes shall communicate the following data to the other Member States through the exchange of supplementary information to all Member States:		1. The Member State which entered the alert into SIS for extradition purposes shall communicate the following data to the other Member States through the exchange of supplementary information to all Member States:	1. The Member State which entered the alert into SIS for extradition purposes shall communicate the following data to the other Member States through the exchange of supplementary information to all Member States:
386	(a) the authority which issued the request for arrest;		(a) the authority which issued the request for arrest;	(a) the authority which issued the request for arrest;

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
387	(b) whether there is an arrest warrant or a document having the same legal effect, or an enforceable judgment;		(b) whether there is an arrest warrant or a document having the same legal effect, or an enforceable judgment;	(b) whether there is an arrest warrant or a document having the same legal effect, or an enforceable judgment;
388	(c) the nature and legal classification of the offence;		(c) the nature and legal classification of the offence;	(c) the nature and legal classification of the offence;
389	(d) a description of the circumstances in which the offence was committed, including the time, place and the degree of participation in the offence by the person for whom the alert has been issued;		(d) a description of the circumstances in which the offence was committed, including the time, place and the degree of participation in the offence by the person for whom the alert has been issued;	(d) a description of the circumstances in which the offence was committed, including the time, place and the degree of participation in the offence by the person for whom the alert has been issued;
390	(e) in so far as possible, the consequences of the offence;		(e) in so far as possible, the consequences of the offence;	(e) in so far as possible, the consequences of the offence;
391	(f) any other information useful or necessary for the execution of the alert.		(f) any other information useful or necessary for the execution of the alert.	(f) any other information useful or necessary for the execution of the alert.
392	2. The data listed in paragraph 1 shall not be communicated where the data referred to in Articles 27 or 28 have already been provided and are considered sufficient for the execution of the alert by the Member State concerned.		2. The data listed in paragraph 1 shall not be communicated where the data referred to in Articles 27 or 28 have already been provided and are considered sufficient for the execution of the alert by the Member State concerned.	2. The data listed in paragraph 1 shall not be communicated where the data referred to in Articles 27 or 28 have already been provided and are considered sufficient for the execution of the alert by the Member State concerned.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
393	*Article 30*	*Article 30*	*Article 30*	*Article 30*
394	*Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes*	*Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes*	*Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes*	*Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes*
395	Where an arrest cannot be made, either because a requested Member State refuses to do so, in accordance with the procedures on flagging set out in Articles 24 or 25, or because, in the case of an alert for arrest for extradition purposes, an investigation has not been completed, the requested Member State shall consider the alert as being an alert for the purposes of communicating the whereabouts of the person concerned.		Where an arrest cannot be made, either because a requested Member State refuses to do so, in accordance with the procedures on flagging set out in Articles 24 or 25, or because, in the case of an alert for arrest for extradition purposes, an investigation has not been completed, the requested Member State shall consider the alert ~~as being an alert~~ for the purposes of communicating the whereabouts of the person concerned.	Where an arrest cannot be made, either because a requested Member State refuses to do so, in accordance with the procedures on flagging set out in Articles 24 or 25, or because, in the case of an alert for arrest for extradition purposes, an investigation has not been completed, the requested Member State shall consider the alert ~~as being an alert~~ for the purposes of communicating the whereabouts of the person concerned.
396	*Article 31*		*Article 31*	*Article 31*
397	*Execution of action based on an alert on a person wanted for arrest with a view to surrender or extradition*		*Execution of action based on an alert on a person wanted for arrest with a view to surrender or extradition*	*Execution of action based on an alert on a person wanted for arrest with a view to surrender or extradition*
398	1. An alert entered in SIS in accordance with Article 26 together with the additional data referred to in Article 27, shall		1. An alert entered in SIS in accordance with Article 26 together with the additional data referred to in Article 27, shall	1. An alert entered in SIS in accordance with Article 26 together with the additional data referred to in Article 27, shall

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	constitute and have the same effect as a European Arrest Warrant issued in accordance with Framework Decision 2002/584/JHA where this Framework Decision applies.		constitute and have the same effect as a European Arrest Warrant issued in accordance with Framework Decision 2002/584/JHA where this Framework Decision applies.	constitute and have the same effect as a European Arrest Warrant issued in accordance with Framework Decision 2002/584/JHA where this Framework Decision applies.
399	2. Where Framework Decision 2002/584/JHA does not apply, an alert entered in SIS in accordance with Articles 26 and 29 shall have the same legal force as a request for provisional arrest under Article 16 of the European Convention on Extradition of 13 December 1957 or Article 15 of the Benelux Treaty concerning Extradition and Mutual Assistance in Criminal Matters of 27 June 1962.		2. Where Framework Decision 2002/584/JHA does not apply, an alert entered in SIS in accordance with Articles 26 and 29 shall have the same legal force as a request for provisional arrest under Article 16 of the European Convention on Extradition of 13 December 1957 or Article 15 of the Benelux Treaty concerning Extradition and Mutual Assistance in Criminal Matters of 27 June 1962.	2. Where Framework Decision 2002/584/JHA does not apply, an alert entered in SIS in accordance with Articles 26 and 29 shall have the same legal force as a request for provisional arrest under Article 16 of the European Convention on Extradition of 13 December 1957 or Article 15 of the Benelux Treaty concerning Extradition and Mutual Assistance in Criminal Matters of 27 June 1962.
400	**CHAPTER VII**		**CHAPTER VII**	
401	**ALERTS ON MISSING PERSONS**		**ALERTS ON MISSING <u>OR</u> VULNERABLE PERSONS**	**ALERTS ON MISSING PERSONS <u>OR VULNERABLE PERSONS WHO NEED TO BE PREVENTED FROM TRAVELLING</u>**
402	*Article 32*	*Article 32*	*Article 32*	*Article 32*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
403	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*
404	1. Data on missing persons or other persons who need to be placed under protection or whose whereabouts need to be ascertained shall be entered in SIS at the request of the competent authority of the Member State issuing the alert.	***deleted***	1. ~~Data on missing persons or other persons who need to be placed under protection or whose whereabouts need to be ascertained shall be entered in SIS at the request of the competent authority of the Member State issuing the alert.~~	***deleted***
405	2. The following categories of missing persons may be entered:	2. The following categories of persons ***shall*** be entered ***in SIS following a decision of the competent authority of the Member State***:	2. The following categories of ~~missing~~ persons **shall**~~may~~ be entered **in SIS at the request of a competent authority of the Member State issuing the alert**:	2. Alerts on the following categories of persons **shall** be entered **in SIS at the request of *the* competent authority of the Member State issuing the alert**:
406	(a) missing persons who need to be placed under protection		(a) missing persons who need to be placed under protection	(a) missing persons who need to be placed under protection
407	(i) for their own protection;		(i) for their own protection;	(i) for their own protection;
408	(ii) in order to prevent threats;	(ii) in order to prevent a threat ***to public security***;	(ii) in order to prevent threats;	(ii) in order to prevent ***a threat to public order or public security;***
409	(b) missing persons who do not need to be placed under protection;	(b) missing ***adults*** who do not need to be placed under protection;	(b) missing persons who do not need to be placed under protection;	(b) missing persons who do not need to be placed under protection;

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
410	(c) children at risk of abduction in accordance with paragraph 4.	(c) children at risk of abduction***, including by a family member, or of being removed from the Member State for the purpose of torture, or sexual or gender-based violence, or of being victims of activities listed in Articles 6 to 10 of Directive 2017/541.***	(c) children at risk of abduction in accordance with paragraph 4 **who need to be prevented from travelling; or**	(c) children at risk of abduction by a parent or a family member, in accordance with paragraph 4, **who need to be prevented from travelling; ~~or~~**
411			**(d) vulnerable persons who need to be prevented from travelling for their own protection in accordance with paragraph 4(a).**	**(ca) ~~vulnerable persons~~ children who need to be prevented from travelling in respect of whom *there is a concrete and apparent risk of them being removed from or leaving the territory of a* Member State and** **(i) becoming victims of trafficking in human beings or victims of forced marriage and or female genital mutilation or other forms of gender-based violence, or** **(ii) becoming victims of or involved in the *offences listed in Articles 6 to 10 of Directive (EU) 2017/541, or***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				(iii)becoming conscripted or enlisted into armed groups or being made to participate actively in hostilities; **(<u>cb</u>) vulnerable persons who are of age who need to be prevented from travelling for their own protection in respect of whom *there is a concrete and apparent risk of them being removed from or leaving the territory of a* Member State and becoming victims of trafficking in human beings or gender-based violence.**
412	3. Paragraph 2(a) shall apply in particular to children and to persons who have to be interned following a decision by a competent authority.	3. Paragraph 2(a) shall apply in particular to persons who have to be interned following a decision by a competent ***judicial*** authority ***and to children***.	3. **<u>Points (a) and (d) of</u>** ~~P~~**<u>p</u>**aragraph 2~~(a)~~ shall apply in particular to children**<u>,</u>** and to **<u>those</u>** persons **<u>in respect of whom</u>** a decision **<u>has been made</u>** by ~~a~~ competent authorit~~y~~**<u>ies</u>**.	3. Point (a) of paragraph 2 shall apply in particular to children and to persons who have to be **<u>institutionalised</u>** following a decision by a competent authority.
413	4. An alert on a child referred to in paragraph 2(c) shall be entered at the request of the competent judicial authority of the Member State that has jurisdiction	4. An alert on a child ***at risk*** referred to in paragraph 2(c) shall be entered ***following a decision*** of the competent judicial authority of the Member State that has jurisdiction in matters of parental	4. An alert on a child referred to in paragraph 2(c) shall be entered at the request of the competent ~~judicial~~ authorit**<u>ies</u>**~~y~~**<u>,including judicial</u>**	4. An alert on a child referred to in paragraph 2(c) shall be entered **following a decision by** the competent authorit**ies, including judicial authorities of the Member States having**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	in matters of parental responsibility in accordance with Council Regulation No 2201/2003[105] where a concrete and apparent risk exists that the child may be unlawfully and imminently removed from the Member State where that competent judicial authority is situated. In Member States which are party to the Hague Convention of 19 October 1996 on Jurisdiction, Applicable law, Recognition, Enforcement and Cooperation in Respect of Parental Responsibility and Measures for the Protection of Children and where Council Regulation No 2201/2003 does not apply, the provisions of the Hague Convention are applicable.	responsibility in accordance with Council Regulation No 2201/2003[106] where a concrete and apparent risk exists that the child may be unlawfully and imminently removed from the Member State where that competent judicial authority is situated. ***Such a decision shall be taken as soon as possible.*** In Member States which are party to the Hague Convention of 19 October 1996 on Jurisdiction, Applicable law, Recognition, Enforcement and Cooperation in Respect of Parental Responsibility and Measures for the Protection of Children and where Council Regulation No 2201/2003 does not apply, the provisions of the Hague Convention are applicable. ***Relevant protocols and tools shall support the necessary action to be taken, as included in the alert.***	**authorities of the Member States having jurisdiction in matters of parental responsibility,** ~~of the Member State that has jurisdiction in matters of parental responsibility in accordance with Council Regulation No 2201/2003[107]~~ where a concrete and apparent risk exists that the child may be unlawfully ~~and imminently~~ removed from the Member State where th~~at~~**e** competent ~~judicial~~ authorit**ies**~~y~~ **are**~~is~~ situated. ~~In Member States which are party to the Hague Convention of 19 October 1996 on Jurisdiction, Applicable law, Recognition, Enforcement and Cooperation in Respect of Parental Responsibility and Measures for the Protection of Children and where Council Regulation No 2201/2003 does not apply, the provisions of the Hague Convention are applicable.~~	**jurisdiction in matters of parental responsibility,** where a concrete and apparent risk exists that the child may be unlawfully and imminently removed from the Member State where th**e** competent authorit**ies are** situated.

[105] Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000 (OJ L 338, 23.12.2003, p. 1).

[106] Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000 (OJ L 338, 23.12.2003, p. 1).

[107] ~~Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000 (OJ L 338, 23.12.2003, p. 1).~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
414			**The competent authority shall regularly review the need to retain the alert.**	*Moved to separate paragraph 4b.*
415		***4a. The competent child protection authorities, including the national hotline and the child's parents, caretakers and/or guardians, as appropriate, taking into account the child's best interests, shall be informed of an alert on a missing child under paragraph 2(c).***	**4a. An alert on vulnerable persons referred to in paragraph 2(d) shall be entered at the request of the competent authorities, where it is considered that a concrete and apparent risk exists to that person should they travel from that Member State.** ~~This shall apply in particular to vulnerable persons in relation to whom it is believed that the travel would create a risk of forced mariage, female genital mutilation, or in the case of minors, of joining armed conflicts, organised criminal groups or terrorist groups.~~	**4a. An alert on persons referred to in paragraph 2 (ca) and (cb) shall be entered following a decision by the competent authorities, including judicial authorities.**
416			**The competent authority shall regularly review the need to retain the alert.**	**4b. The ~~competent authority~~ issuing Member State shall regularly review the need to retain the alerts referred to in paragraph 2(c), (ca) and (cb) in accordance with Article 51(3)**
417	5. Member States shall ensure that the data entered in SIS indicate which of the categories referred to in paragraph 2 the missing person	5. Member States shall ensure that the data entered in SIS indicate which of the categories referred to in paragraph 2 the missing person	5. Member States shall ensure that the data entered in SIS indicate which of the categories referred to in paragraph 2 the ~~missing~~ person	5. Member States shall ensure that the data entered in SIS indicate which of the categories referred to in paragraph 2 the person falls into.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	falls into. Further, Member States shall also ensure that the data entered in SIS indicate which type of missing or vulnerable person case is involved. The rules on the categorisation of the types of cases and the entering of such data shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	or ***child at risk*** falls into. Further, Member States shall also ensure that the data entered in SIS indicate which type of ***child at risk or*** missing person case is involved***, wherever the type of case is known***. The rules on the categorisation of the types of cases and the entering of such data shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2). ***Under those rules, the types of missing persons who are children shall include:***	falls into. Further, Member States shall also ensure that the data entered in SIS indicate which type of ~~missing or vulnerable person~~ case is involved **and that, in relation to alerts issued pursuant to points (c) and (d) of paragraph 2, all relevant information is made available at the SIRENE Bureau of the issuing Member State at the time of the alert creation**. ~~The rules on the categorisation of the types of cases and the entering of such data shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[108]	Member States shall also ensure that the data entered in SIS indicate which type of case is involved**, *wherever the type of case is known*, and that, in relation to alerts issued pursuant to points (c), (ca) and (cb) of paragraph 2, all relevant information is made available at the SIRENE Bureau of the issuing Member State at the time of the alert's creation**.
418		***(a) runaways;***		
419		***(b) unaccompanied children in the context of migration;***		
420		***(c) children abducted by a family member.***		
421	6. Four months before a child who is the subject of an alert under this Article reaches adulthood, CS-SIS shall automatically notify the	6. Four months before a child who is the subject of an alert under this Article reaches adulthood, CS-SIS shall automatically notify the	6. Four months before a child who is the subject of an alert under this Article reaches **the age of majority in accordance with the**	6. Four months before a child who is the subject of an alert under this Article reaches **the age of majority in accordance with the**

[108] Moved to paragraph 8.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	issuing Member State that the reason for request and the action to be taken have to be updated or the alert has to be deleted.	issuing Member State that the reason for request and the action to be taken have to be updated or the alert ***will*** be deleted	**national law of the issuing Member State**~~adulthood~~, CS-SIS shall automatically notify the issuing Member State that the reason for request and the action to be taken have to be updated or the alert has to be deleted.	**national law of the issuing Member State**, CS-SIS shall automatically notify the issuing Member State that the reason for request and the action to be taken have to be updated or the alert has to be deleted.
422	7. Where there is a clear indication that vehicles, boats or aircraft are connected with a person who is the subject of an alert pursuant to paragraph 2, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In those cases the alert on the missing person and the alert on the object shall be linked in accordance with Article 60. The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	7. Where there is a clear indication that vehicles, boats or aircraft are connected with a person who is the subject of an alert pursuant to paragraph 2, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In those cases the alert on the person and the alert on the object shall be linked in accordance with Article 60. The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	7. Where there is a clear indication that vehicles, boats or aircraft are connected with a person who is the subject of an alert pursuant to paragraph 2, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In those cases the alert on the ~~missing~~ person and the alert on the object shall be linked in accordance with Article 60. ~~The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[109]	7. Where there is a clear indication that vehicles, boats or aircraft are connected with a person who is the subject of an alert pursuant to paragraph 2, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In those cases the alert on the person and the alert on the object shall be linked in accordance with Article 60.
423		***7a. Member States shall enter in SIS the data of children who***		moved to recital 23A

[109] Moved to paragraph 8.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		have gone missing from reception facilities as missing persons.		
424			**8.**[110] **The Commission shall adopt implementing acts to lay down and develop rules on the categorisation of the types of cases and the entering of data referred to in paragraph 5 and technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 7. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**	**8.**[111] **The Commission shall adopt implementing acts to lay down and develop rules on the categorisation of the types of cases and the entering of data referred to in paragraph 5. The *types of cases of missing persons who are children shall include, but not be limited to,* runaways, unaccompanied children in the context of migration and ~~abducted~~ children** at risk of parental abduction**.** **The Commission shall also adopt implementing acts to lay down and develop technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 7.** **Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**
425	*Article 33*	*Article 33*	*Article 33*	*Article 33*

[110] Moved from paragraph 5 *in fine* and paragraph 7 *in fine*.
[111] Moved from paragraph 5 *in fine* and paragraph 7 *in fine*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				Text of this Article is the informal outcome of technical discussion to be confirmed by trilogue
426	*Execution of action based on an alert*	*Execution of action based on an alert*	*Execution of action based on an alert*	*Execution of action based on an alert*
427	1. Where a person as referred to in Article 32 is located, the competent authorities shall, subject to paragraph 2, communicate his or her whereabouts to the Member State issuing the alert. In the case of missing children or children who need to be placed under protection the executing Member State shall consult immediately the issuing Member State in order to agree without delay on the measures to be taken in order to safeguard the best interest of the child. The competent authorities may, in the cases referred to in Article 32(2)(a) and (c), move the person to a safe place in order to prevent him or her from continuing his journey, if so authorised by national law.	1. Where a person as referred to in Article 32 is located, the competent authorities shall, ***without prejudice*** to paragraph 2, communicate ***without delay*** his or her whereabouts to the Member State issuing the alert. In the case of children ***subject to alerts under Article 32*** the executing Member State shall consult ***without delay*** the issuing Member State ***including its child protection authorities*** in order to agree without delay ***and at the latest within 12 hours*** on the measures to be taken in order to safeguard the best interest of the child. The competent authorities may, ***where appropriate,*** in the cases referred to in Article 32(2)(a) and (c), move the person to a safe place in order to prevent him or her from continuing his journey, if so authorised by national law. ***If the alert concerns a child, the decision on the safe place shall***	1. Where a person as referred to in Article 32 is located, the competent authorities shall, subject to paragraph 2, communicate his or her whereabouts to the Member State issuing the alert.	1. Where a person referred to in Article 32 is located, the competent authorities shall, **subject to the requirements in** paragraph 2, communicate his or her whereabouts to the Member State issuing the alert.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		take in consideration the vulnerability of the child and his or her best interests.		
428			**1a.** In the case of **persons** ~~missing children or children~~ who need to be placed under protection **as referred to in Article 32(2)(a), (c) and (d),** the executing Member State shall ~~consult~~ immediately **consult its own competent authorities and those in** the issuing Member State **through the exchange of supplementary information** in order to agree without delay on the measures to be taken in order to safeguard the best interest of the child. The competent authorities **in the executing Member State** may**, in accordance with national law,** ~~, in the cases referred to in Article 32(2)(a) and (c),~~ move the person to a safe place in order to prevent him or her from continuing his journey~~, if so authorised by national law~~.	**1a.** In the case of **persons** who need to be placed under protection **as referred to in Article 32(2)(a), (c), ~~and~~ (ca) and (cb),** the executing Member State shall immediately **consult its own competent authorities and those of** the issuing Member State **through the exchange of supplementary information** in order to agree without delay on the measures to be taken. The competent authorities **in the executing Member State** may**, in accordance with national law,** move ***such persons*** to a safe place in order to prevent them from continuing their journey.
429				1b. **In the case of children any decision on the measures to be taken or any decision to move ~~him or her~~** the child **to a safe place as**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				referred to in paragraph 1a *shall be made in accordance with* the best interests of the child**. Such decisions shall be made** immediately and not later than**~~within~~ 12 hours of when the child is located in consultation with relevant child protection authorities, as appropriate**.
430	2. The communication, other than between the competent authorities, of data on a missing person who has been located and who is of age shall be subject to that person's consent. The competent authorities may, however, communicate the fact that the alert has been erased because the missing person has been located to the person who reported the person missing.		2. The communication, other than between the competent authorities, of data on a missing person who has been located and who is of age shall be subject to that person's consent. The competent authorities may, however, communicate the fact that the alert has been erased because the missing person has been located to the person who reported the person missing.	2. The communication, other than between the competent authorities, of data on a missing person who has been located and who is of age shall be subject to that person's consent. The competent authorities may, however, communicate the fact that the alert has been erased because the missing person has been located to the person who reported the person missing.
431	**CHAPTER VIII**	**CHAPTER VIII**	**CHAPTER VIII**	**CHAPTER VIII**
432	**ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE**	**ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE**	**ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE**	**ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE**
433	*Article 34*	*Article 34*	*Article 34*	*Article 34*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
434	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*
435	1. For the purposes of communicating the place of residence or domicile of persons, Member States shall, at the request of a competent authority, enter in SIS data on:		1. For the purposes of communicating the place of residence or domicile of persons, Member States shall, at the request of a competent authority, enter in SIS data on:	1. For the purposes of communicating the place of residence or domicile of persons, Member States shall, at the request of a competent authority, enter in SIS data on:
436	(a) witnesses;		(a) witnesses;	(a) witnesses;
437	(b) persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted;		(b) persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted;	(b) persons summoned or persons sought to be summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted;
438	(c) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted;		(c) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted;	(c) persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings in order to account for acts for which they are being prosecuted;
439	(d) persons who are to be served with a summons to report in order to serve a penalty		(d) persons who are to be served with a summons to report in order to serve a penalty	(d) persons who are to be served with a summons to report in order to serve a penalty

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	involving deprivation of liberty.		involving deprivation of liberty.	involving deprivation of liberty.
440	2. Where there is a clear indication that vehicles, boat or aircraft are connected with a person subject of an alert pursuant to paragraph 1, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In such cases the alerts on the person and the alert on the object shall be linked in accordance with Article 60. The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).		2. Where there is a clear indication that vehicles, boat**s** or aircraft are connected with a person subject of an alert pursuant to paragraph 1, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In such cases the alerts on the person and the alert on the object shall be linked in accordance with Article 60. ~~The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2)~~[112].	2. Where there is a clear indication that vehicles, boat**s** or aircraft are connected with a person subject of an alert pursuant to paragraph 1, alerts on those vehicles, boats and aircraft may be issued in order to locate the person. In such cases the alerts on the person and the alert on the object shall be linked in accordance with Article 60.
441			**3.**[113] **The Commission shall adopt implementing acts to lay down and develop technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2. Those**	**3.**[114] **The Commission shall adopt implementing acts to lay down and develop technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2. Those**

[112] Moved to paragraph 3.
[113] Moved from paragraph 2, *in fine*.
[114] Moved from paragraph 2, *in fine*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).	**implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**
442	*Article 35*	*Article 35*	*Article 35*	*Article 35*
443	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*
444	Requested information shall be communicated to the requesting Member State through the exchange of supplementary information.		Requested information shall be communicated to the requesting Member State through the exchange of supplementary information.	Requested information shall be communicated to the requesting Member State through the exchange of supplementary information.
445	**CHAPTER IX**	**CHAPTER IX**	**CHAPTER IX**	**CHAPTER IX**
446	**ALERTS ON PERSONS AND OBJECTS FOR DISCREET CHECKS, INQUIRY CHECKS OR SPECIFIC CHECKS**	**ALERTS ON PERSONS AND OBJECTS FOR DISCREET CHECKS, INQUIRY CHECKS OR SPECIFIC CHECKS**	**ALERTS ON PERSONS AND OBJECTS FOR DISCREET CHECKS, INQUIRY CHECKS OR SPECIFIC CHECKS**	**ALERTS ON PERSONS AND OBJECTS FOR DISCREET CHECKS, INQUIRY CHECKS OR SPECIFIC CHECKS**
447	*Article 36*	*Article 36*	*Article 36*	*Article 36* *Provisionally agreed at political trilogue on 12 April 2018 subject to further fine-tuning at technical level*
448	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
449	1. Data on persons or vehicles, boats, aircraft and containers shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet checks, inquiry checks or specific checks in accordance with Article 37(4).		1. Data on persons or **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (j), (k) and non-cash means of payment** shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet checks, inquiry checks or specific checks in accordance with Article 37**(3),** (4) **and (5)**.	1. Data on persons**, on** ~~or~~ **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (j), (k) and on non-cash means of payment** shall be entered in accordance with the national law of the Member State issuing the alert, for the purposes of discreet checks, inquiry checks or specific checks in accordance with Article 37**(3),** (4) **and (5)**.
450			**1a. When issuing alerts for the purposes of discreet checks, inquiry checks or specific checks and where the information sought by the issuing Member State is additional to that provided for in Article 37(1), the issuing Member State shall add to the alert all information being sought.**	**1a. When issuing alerts for the purposes of discreet checks, inquiry checks or specific checks and where the information sought by the issuing Member State is additional to that provided for in Article 37(1)(a) to (h), the issuing Member State shall add to the alert all information being sought.**
451	2. The alert may be issued for the purposes of prosecuting criminal offences, executing a criminal sentence and for the prevention of threats to public security:	2. The alert may be issued for the purposes of ***preventing, detecting, investigating and*** prosecuting criminal offences, executing a criminal sentence and for the prevention of threats to public security:	2. The alert may be issued for the purposes of **preventing, detecting, investigating or** prosecuting criminal offences, executing a criminal sentence and for the prevention of threats to public security:	2. The alert may be issued for the purposes of **preventing, detecting, investigating or** prosecuting criminal offences, executing a criminal sentence and for the prevention of threats to public security:

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
452	(a) where there is a clear indication that a person intends to commit or is committing a serious crime, in particular the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA;	(a) where there is clear indication that a person intends to commit or is committing a serious crime***, where this is punishable, in the issuing Member State, by a custodial sentence or detention order for a maximum period of at least one year***;	(a) where there is a clear indication that a person intends to commit or is committing a serious crime, in particular the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; **or**	(a) where there is a clear indication that a person intends to commit or is committing ~~a serious crime, in particular~~ **any of the** offences referred to in Article **2(1) and** (2) of the Framework Decision 2002/584/JHA; **or**
453	(b) where the information referred to in Article 37(1) is necessary for the execution of a criminal sentence of a person convicted of a serious crime, in particular the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; or	(b) where the information referred to in Article 37(1) is necessary for the execution of a criminal sentence of a person convicted of a serious crime***, where this is punishable, in the issuing Member State, by a custodial sentence or detention order for a maximum period of at least three years***; or	(b) where the information referred to in Article 37(1) is necessary for the execution of a criminal ~~sentence~~ **penalty** of a person convicted of a serious crime, in particular the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA; or	(b) where the information referred to in Article 37(1) is necessary for the execution of a ~~criminal sentence~~ **penalty *custodial sentence or detention order regarding*** ~~of~~ a person convicted ~~of a serious crime, in particular~~ **of any of** the offences referred to in Article 2(**1) and** (2) of the Framework Decision 2002/584/JHA; or
454	(c) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may also commit serious crimes in the future, in particular the offences referred to in Article	(c) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may also commit serious crimes in the future***, where this is punishable, in the issuing Member State, by a custodial sentence or detention***	(c) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may also commit serious crimes in the future, in particular the offences referred to in Article	(c) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may also commit ~~serious crimes~~ in the future~~, in particular~~ the offences referred to in Article **2(1) and** 2(2) of the

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	2(2) of the Framework Decision 2002/584/JHA.	***order for a maximum period of at least three years***.	2(2) of the Framework Decision 2002/584/JHA.	Framework Decision 2002/584/JHA.
455	3. In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is a concrete indication that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Member State issuing the alert pursuant to this paragraph shall inform the other Member States thereof. Each Member State shall determine to which authorities this information shall be transmitted.		3. In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is a concrete indication that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Member State issuing the alert pursuant to this paragraph shall inform the other Member States thereof. Each Member State shall determine to which authorities this information shall be transmitted **via its SIRENE Bureau**.	3. In addition, an alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is a concrete indication that the information referred to in Article 37(1) is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Member State issuing the alert pursuant to this paragraph shall inform the other Member States thereof. Each Member State shall determine to which authorities this information shall be transmitted **via its SIRENE Bureau**.
456	4. Where there is a clear indication that vehicles, boats, aircraft and containers are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those vehicles, boats, aircraft and containers may be issued.	4. Where there is clear ***evidence*** that vehicles, boats, aircraft, containers***, trailers with an unladen weight exceeding 750 kg and caravans*** are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those vehicles, boats, aircraft and containers may be	4. Where there is a clear indication that **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (j), (k) or non-cash means of payment**~~vehicles, boats, aircraft and containers~~ are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those **objects** ~~vehicles, boats,~~	4. Where there is a clear indication that **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), [(i)], (j), (k) or non-cash means of payment** are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those **objects** may be issued **and**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		issued.	~~aircraft and containers~~ may be issued **and linked to the alerts inserted pursuant to paragraphs 2 and 3**.	**linked to the alerts entered pursuant to paragraphs 2 and 3**.
457	5. Where there is a clear indication that blank official documents or issued identity documents are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those documents, regardless of the identity of the original holder of the identity document, if any, may be issued. The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	5. Where there is clear ***evidence*** that blank official documents or issued identity documents are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those documents, regardless of the identity of the original holder of the identity document, if any, may be issued. The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	5. ~~Where there is a clear indication that blank official documents or isued identity documents are connected with the serious crimes referred to in paragraph 2 or the serious threats referred to in paragraph 3, alerts on those documents, regardless of the identity of the original holder of the identity document, if any, may be issued. The technical rules necessary for entering, updating, deleting and searching the data referred to in this paragraph shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).~~[115]	***(deletion)***
458			**6.**[116] **The Commission shall adopt implementing acts to lay down and develop the technical rules necessary for entering,**	**6.**[117] **The Commission shall adopt implementing acts to lay down and develop the technical rules necessary for entering,**

[115] Moved to paragraph 6.
[116] Moved from paragraph 5 *in fine*.
[117] Moved from paragraph 5 *in fine*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			updating, deleting and searching the data referred to in paragraph 4 as well as the additional information referred to in paragraph 1a. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).	**updating, deleting and searching the data referred to in paragraph 4 [as well as the additional information referred to in paragraph 1a]. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 72(2).**
459	*Article 37*	*Article 37*	*Article 37*	*Article 37* *Provisionally agreed at political trilogue on 12 April 2018 subject to further fine-tuning at technical level*
460	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*
461	1. For the purposes of discreet checks, inquiry checks or specific checks, all or some of the following information shall be collected and communicated to the authority issuing the alert when border control checks, police and customs checks or other law enforcement activities are carried out within a Member State:	1. For the purposes of discreet checks, inquiry checks or specific checks, all or some of the following information shall be collected and ***immediately*** communicated to the authority issuing the alert when border control checks, police and customs checks or other law enforcement activities are carried out within a Member State:	1. For the purposes of discreet checks, inquiry checks or specific checks, all or some of the following information shall be collected and communicated to the ~~authority~~ issuing ~~the alert when border control checks, police and customs checks or other law enforcement activities are carried out within a~~ Member State:	1. For the purposes of discreet checks, inquiry checks or specific checks, all or some of the following information shall be collected and communicated to the issuing Member State:
462	(a) the fact that the person for whom, or the vehicle, boat,		(a) the fact that the person for whom, or the **objects**	(a) the fact that the person **who is the subject of an alert has**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	aircraft, container, blank official document or issued identity paper for which an alert has been issued, has been located;		**referred to in Article**~~vehicle, boat, aircraft, container, blank official document or issued identity paper~~ **38(2)(a), (b), (c), (e), (g), (h), (j), (k) or non-cash means of payment** for which an alert has been issued, has **or have** been located;	**been located**, or **that objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), [(i),] (j), (k) or non-cash means of payment** which **are the subject of** an alert **have** been located;
463	(b) the place, time and reason for the check;		(b) the place, time and reason for the check;	(b) the place, time and reason for the check;
464	(c) the route of the journey and destination ;		(c) the route of the journey and destination ;	(c) the route of the journey and destination ;
465	(d) the persons accompanying the person concerned or the occupants of the vehicle, boat or aircraft or accompanying the holder of the blank official document or issued identity document who can reasonably be expected to be associated with the persons concerned;		(d) the persons accompanying the person concerned or the occupants of the vehicle, boat or aircraft or accompanying the holder of the blank official document or issued identity document who can reasonably be expected to be associated with the persons concerned;	(d) the persons accompanying the person concerned or the occupants of the vehicle, boat or aircraft or accompanying the holder of the blank official document or issued identity document who can reasonably be expected to be associated with the persons concerned;
466	(e) the identity revealed and personal description of the person using the blank official document or issued		(e) the identity revealed and personal description of the person using the blank official document or issued	(e) the identity revealed and personal description of the person using the blank official document or issued

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	identity paper subject of the alert;		identity paper subject of the alert;	identity paper subject of the alert;
467	(f) the vehicle, boat, aircraft or container used;	(f) the vehicle, boat, aircraft, container, ***trailers with an unladen weight exceeding 750 kg and caravans*** used;	(f) **objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), (j), (k) or non-cash means of payment** ~~the vehicle, boat, aircraft or container~~ used;	(f) **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), [(i)], (j), (k) or non-cash means of payment** used;
468	(g) objects carried, including travel documents;		(g) objects carried, including travel documents;	(g) objects carried, including travel documents;
469	(h) the circumstances under which the person or the vehicle, boat, aircraft, container, blank official document or issued identity paper was located.		(h) the circumstances under which the person or the **motor** vehicle, **trailer, caravan,** boat, **container,** aircraft, ~~container,~~ blank official document or issued identity ~~paper~~**documents or non-cash means of payment** was located**;**	(h) the circumstances under which the person or **the objects referred to in Article 38(2)(a), (b), (c), (e), (g), (h), [(i),] (j), (k) or non-cash means of payment** was located**;**
470			**(i) other information, the collection of which may have been requested by the issuing Member State in accordance with Article 36(1a)**.	To be further discussed *Informal outcome of technical discussion awaiting feedback from respective Legal Services:* **(i) any other information being sought by the issuing Member State in accordance with Article 36(1a)**.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				If the information referred to under point (i) relates to data categories defined in Article 10 of Directive (EU) 2016/680, such information may only be sought where strictly necessary for the specific purpose of the alert and processed in accordance with the conditions set out pursuant to that Article [and...].
471	2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.	2. The information referred to in paragraph 1 shall be ***immediately*** communicated through the exchange of supplementary information.	2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.	2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.
472	3. Depending on the operational circumstances and in accordance with national law, a discreet check shall comprise a routine check of a person or object with a view to collecting as much of the information described in paragraph 1 as possible without jeopardising the discreet nature of the check.		3. ~~Depending on the operational circumstances and in accordance with national law, a~~**A** discreet check shall comprise **the discreet collection of as much information described in paragraph 1 as possible during routine activities carried out by the competent national authorities**. **The collection of this information shall not jeopardise the discreet nature of the checks and the subject of the alert shall**	**3. A** discreet check shall comprise **the discreet collection of as much information described in paragraph 1 as possible during routine activities carried out by the competent national authorities**. **The collection of this information shall not jeopardise the discreet nature of the checks and the subject of the alert shall in no way be made aware of the existence of the alert.**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			in no way be made aware as to the existence of the alert.	
473	4. Depending on the operational circumstances and in accordance with national law, an inquiry check shall comprise a more in-depth check and a questioning of the person. Where inquiry checks are not authorised by the law of a Member State, they shall be replaced by discreet checks in that Member State.	4. Depending on the operational circumstances and in accordance with national law, ***and without prejudice to the rights of suspects and accused persons to have access to a lawyer in accordance with Directive 2013/48/EU of the European Parliament and of the Council[118],*** an inquiry check shall comprise a more in-depth check and a questioning of the person.	4. ~~Depending on the operational circumstances and in accordance with national law~~**A**n inquiry check shall comprise **the** ~~a more in-depth check and a questioning~~ **interviewing** of the person~~. Where inquiry checks are not authorised by the law of a Member State, they shall be replaced by discreet checks in that Member State~~[119]**, including on the basis of information or specific questions added to the alert by the issuing Member State. The interview shall be carried out in accordance with the national law of the executing Member State.** ~~The person may be informed about the alert or the issuing authority.~~	4. An inquiry check shall comprise **the interviewing** of the person**, including on the basis of information or specific questions added to the alert by the issuing Member State. The interview shall be carried out in accordance with the national law of the executing Member State[120].**
474	5. During specific checks, persons, vehicles, boats, aircraft,		5. During specific checks, persons, vehicles, boats, aircraft,	5. During specific checks, persons, vehicles, boats, aircraft,

[118] ***Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294, 6.11.2013, p. 1).***

[119] Moved to new paragraph 6.

[120] ***Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294, 6.11.2013, p. 1).***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	containers and objects carried, may be searched in accordance with national law for the purposes referred to in Article 36. Searches shall be carried out in accordance with national law. Where specific checks are not authorised by the law of a Member State, they shall be replaced by inquiry checks in that Member State.		containers and objects carried, may be searched ~~in accordance with national law~~ for the purposes referred to in Article 36. Searches shall be carried out in accordance with national law. ~~Where specific checks are not authorised by the law of a Member State, they shall be replaced by inquiry checks in that Member State.~~[121]	containers and objects carried, may be searched for the purposes referred to in Article 36. Searches shall be carried out in accordance with national law.
475			**6.** Where specific checks are not authorised by ~~the~~ **national** law ~~of a Member State~~, they shall be replaced by inquiry checks in that Member State[122]. **Where inquiry checks are not authorised by national law, they shall be replaced by discreet checks in that Member State**[123]**.**	Presidency compromise proposal**:** **6.** Where specific checks are not authorised by ~~the~~ **national** law ~~of a Member State~~, they shall be replaced by inquiry checks in that Member State. **Where inquiry checks are not authorised by national law, they shall be replaced by discreet checks in that Member State. *Where Directive 2013/48 applies , Member States shall ensure that the right of suspects and accused persons to have access to a lawyer is respected under the conditions set out in that Directive*.**

121 Moved to new paragraph 6.
122 Moved from paragraph 5.
123 Moved from paragraph 4.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
476			**7. Paragraph 6 is without prejudice to the obligation of Member States to make available to the end-users all additional information referred to in Article 36(1a) and to ensure that this information is collected and communicated to the issuing Member State through the exchange of supplementary information.**	**7. Paragraph 6 is without prejudice to the obligation of Member States to make available to the end-users the information soughtunder Article 36(1a).**
477	**CHAPTER X**	**CHAPTER X**	**CHAPTER X**	**CHAPTER X**
478	**ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS**	**ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS**	**ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS**	**ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS**
479	*Article 38*	*Article 38*	*Article 38*	*Article 38*
480	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*	*Objectives and conditions for issuing alerts*
481	1. Data on objects sought for the purposes of seizure for law enforcement purposes or use as evidence in criminal proceedings shall be entered in SIS.		1. Data on objects sought for the purposes of seizure ~~for law enforcement purposes~~ or **for** use as evidence in criminal proceedings shall be entered in SIS.	1. Data on objects sought for the purposes of seizure ~~for law enforcement purposes~~ or **for** use as evidence in criminal proceedings shall be entered in SIS.
482	2. The following categories of readily identifiable objects shall be entered:		2. The following categories of readily identifiable objects shall be entered:	2. The following categories of readily identifiable objects shall be entered:

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
483	(a) motor vehicles, as defined by national law, regardless of the propulsion system;		(a) motor vehicles~~, as defined by national law,~~ regardless of the propulsion system;	(a) motor vehicles~~, as defined by national law,~~ regardless of the propulsion system;
484	(b) trailers with an unladen weight exceeding 750 kg;		(b) trailers with an unladen weight exceeding 750 kg;	(b) trailers with an unladen weight exceeding 750 kg;
485	(c) caravans;		(c) caravans;	(c) caravans;
486	(d) industrial equipment;		(d) industrial equipment;	(d) industrial equipment;
487	(e) boats;		(e) boats;	(e) boats;
488	(f) boat engines;		(f) boat engines;	(f) boat engines;
489	(g) containers;		(g) containers;	(g) containers;
490	(h) aircraft;	(h) aircraft ***and aircraft engines***;	(h) aircraft;	(h) aircraft;
491			**(ha) aircraft engines;**	**(ha) aircraft engines;**
492	(i) firearms;		(i) firearms;	(i) firearms;
493	(j) blank official documents which have been stolen, misappropriated or lost;		(j) blank official documents which have been stolen, misappropriated**,** ~~or~~ lost **or purport to be such a document but are false**;	*Provisionally agreed subject to lawyer linguists' feedback on terminology* (j) blank official documents which have been stolen, misappropriated**,** ~~or~~ lost **or purport to be such a document but are false**;

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
494	(k) issued identity documents such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or, invalidated or purport to be such a document but are falsified;		(k) issued identity documents such as passports, identity cards, ~~driving licenses,~~ residence permits**,** ~~and~~ travel documents and **as well as driving licenses** which have been stolen, misappropriated, lost or, invalidated or purport to be such a document but are fals~~ified~~;	*Provisionally agreed subject to lawyer linguists' feedback on terminology* (k) issued identity documen ts - such as passports, identity cards, ~~driving licenses,~~ residence permits**,** ~~and~~ travel documents ~~and~~ **and driving licences -** which have been stolen, misappropriated, lost or, invalidated or purport to be such a document but are ***false***;
495	(l) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost, or invalidated or purport to be such a document or plate but are falsified;		(l) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost, or invalidated or purport to be such a document or plate but are fals~~ified~~;	*Provisionally agreed subject to lawyer linguists' feedback on terminology* (l) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost, or invalidated or purport to be such a document or plate but are ***false***;
496	(m) banknotes (registered notes) and falsified banknotes;		(m) banknotes (registered notes) and fals~~ified~~ banknotes;	*Provisionally agreed subject to lawyer linguists' feedback on terminology* (m) banknotes (registered notes) and ***false*** banknotes;

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
497	(n) technical equipment, information technology items and other high-value readily identifiable objects;		(n) ~~technical equipment,~~information technology items ~~and other high value readily identifiable objects~~[124];	(n) ~~technical equipment,~~information technology items ~~and other high value readily identifiable objects~~[125];
498	(o) identifiable component parts of motor vehicles;		(o) identifiable component parts of motor vehicles;	(o) identifiable component parts of motor vehicles;
499	(p) identifiable component parts of industrial equipment.		(p) identifiable component parts of industrial equipment**;**	(p) identifiable component parts of industrial equipment**;**
500			**(q) other identifiable objects of high-value**[126]**, as defined in accordance with paragraph 3**.	**(q) other identifiable objects of high-value**[127]**, as defined in accordance with paragraph 3**.
501			**With regard to the documents referred to in paragraphs 2(j), (k) and (l), the issuing Member State may specify whether such documents are stolen, misappropriated, lost, invalidated or false.**	*Provisionally agreed subject to lawyer linguists' feedback on terminology* **With regard to the documents referred to in points (j), (k) and (l), the issuing Member State may specify whether such documents are stolen, misappropriated, lost, invalid or false.**

124 Moved to new point (q).
125 Moved to new point (q).
126 Moved from point (n).
127 Moved from point (n).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
502	3. The definition of new sub-categories of object under paragraph 2(n) and the technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	3. The ***Commission shall be empowered to adopt a delegated act in accordance with Article 71a to define*** new sub-categories of object under paragraph 2(n)***. The*** technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	3. The definition of new sub-categories of object**s** under paragraph 2(n)**, (o), (p) and (q)** and the technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).	Rapporteur's proposal: 3. The ***Commission shall be empowered to adopt a delegated act in accordance with Article 71a to define*** new sub-categories of object**s** under paragraph 2(n)**, (o), (p) and (q).**
503				**4.** The technical rules necessary for entering, updating, deleting and searching the data referred to in paragraph 2 shall be laid down and developed by means of implementing measures in accordance with the examination procedure referred to in Article 72(2).
504	*Article 39*	*Article 39*	*Article 39*	*Article 39*
505	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*
506	1. Where a search brings to light an alert for an object which	1. Where a search brings to light an alert for an object which has been located, the authority	1. Where a search brings to light an alert for an object which	1. Where a search brings to light an alert for an object which

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	has been located, the authority which matched the two items of data shall in accordance with national law seize the object and contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated in accordance with this Regulation.	which matched the two items of data shall in accordance with national law seize the object and contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated ***through the exchange of supplementary information***.	has been located, the authority which matched the two items of data shall in accordance with national law seize the object and contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated in accordance with this Regulation.	has been located, the authority which matched the two items of data shall in accordance with national law seize the object and contact the authority which issued the alert in order to agree on the measures to be taken. For this purpose, personal data may also be communicated in accordance with this Regulation.
507	2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.	***deleted***	2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.	2. The information referred to in paragraph 1 shall be communicated through the exchange of supplementary information.
508	3. The Member State which located the object shall take the requested measures in accordance with national law.		3. The Member State which located the object shall take the requested measures in accordance with national law.	3. The Member State which located the object shall take the requested measures in accordance with national law.
509	**CHAPTER XI**	**CHAPTER XI**	**CHAPTER XI**	**CHAPTER XI**
510	**ALERTS ON UNKNOWN WANTED PERSONS FOR IDENTIFICATION ACCORDING TO NATIONAL LAW AND SEARCH WITH BIOMETRIC DATA**	ALERTS ON UNKNOWN WANTED PERSONS FOR ***IDENTIFICATION UNDER*** NATIONAL LAW	**ALERTS ON UNKNOWN WANTED PERSONS FOR IDENTIFICATION ACCORDING TO NATIONAL LAW ~~AND SEARCH WITH BIOMETRIC DATA~~**[128]	**ALERTS ON UNKNOWN WANTED PERSONS FOR IDENTIFICATION UNDER NATIONAL LAW**

[128] Moved to new Chapter XIa.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
511	*Article 40*	*Article 40*	*Article 40*	*Article 40*
512	*Alerts on unknown wanted person for apprehension under national law*	*Alerts on unknown wanted person for **identification** under national law*	*Alerts on unknown wanted person for ~~apprehension~~ **identification** under national law*	*Alerts on unknown wanted person for **identification** under national law*
513	Dactylographic data may be entered in SIS, not related to persons who are subject of the alerts. These dactylographic data shall be either complete or incomplete sets of fingerprints or palm prints discovered at the scenes of crimes under investigation, of serious crime and terrorist offence and where it can be established to a high degree of probability that they belong to the perpetrator of the offence. The dactylographic data in this category shall be stored as "unknown suspect or wanted person" provided that the competent authorities cannot establish the identity of the person by using any other national, European or international database.	1. ***Dactyloscopic*** data may be entered in SIS, not related to persons who are subject of the alerts. These ***dactyloscopic*** data shall be either complete or incomplete sets of fingerprints or palm prints discovered at the scenes of terrorist ***offences or other serious crimes under investigation*** and where it can be established to a ***very*** high degree of probability that they belong to the perpetrator of the offence. ***If the competent authority of the issuing Member State cannot establish the identity of the suspect by using any other relevant data base, the dactyloscopic data in this category may be stored as "unknown suspect or wanted person" for the purpose of identifying such a person and his or her whereabouts.***	Dactylo**sco**~~graph~~ic data may be entered in SIS, not related to persons who are subject of the alerts. These dactylo**sco**~~graph~~ic data shall be either complete or incomplete sets of fingerprints or palm prints **that are** discovered at the scenes of **serious** crimes **or terrorist offences** under investigation, ~~of serious crime and terrorist offence~~ and where it can be established to a high degree of probability that they belong to ~~the~~ **a** perpetrator of the offence. The dactylo**sco**~~graph~~ic data in this category shall be stored as "unknown suspect or wanted person" **and shall only be stored where**~~provided that~~ the competent authorities **of the issuing Member State** cannot establish the identity of the person by using any other national, European or international database.	*LIBE proposal:* 1. ***Dactyloscopic*** data ***which is un***related to persons who are ***the*** subject of alerts ***may be entered into SIS***. These ***dactyloscopic*** data shall be either complete or incomplete sets of fingerprints or palm prints discovered at the scenes of terrorist ***offences or other serious crimes under investigation. They shall only be entered into SIS*** where it can be established to a ***very*** high degree of probability that they belong to **a** perpetrator of the offence. ***If the competent authority of the issuing Member State cannot establish the identity of the suspect on the basis of data from any other relevant*** national, ***Union*** or international database***, the dactyloscopic data referred to in the first subparagraph may only be stored in this category of alerts as "unknown wanted person" for the***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				purpose of identifying such a person.
514	*Article 41*	*Article 41*	*Article 41*	*Article 41*
515	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*	*Execution of the action based on an alert*
516	In the event of a hit or a potential match with the data stored pursuant to Article 40, the identity of the person shall be established in accordance with national law, together with verification that the dactylographic data stored in SIS belong to the person. Member States shall communicate by using supplementary information in order to facilitate timely investigation of the case.	1. In the event of a hit or a potential match with the data stored pursuant to Article 40, the identity of the person shall be established in accordance with national law, ***after*** verification ***by a fingerprint expert*** that the ***dactyloscopic*** data stored in SIS belong to the person.Member States shall ***immediately*** communicate by using supplementary information in order to facilitate timely investigation of the case.	In the event of a hit ~~or a potential match~~ with the data stored pursuant to Article 40, the identity of the person shall be established in accordance with national law, together with **expert** verification that the dactylo**sco**~~graph~~ic data stored in SIS belong to the person. Member States shall communicate **information about the identity and the whereabouts of the person** ~~by using~~**through the exchange of** supplementary information in order to facilitate timely investigation of the case.	In the event of a hit with the data stored pursuant to Article 40, the identity of the person shall be established in accordance with national law, together with **expert** verification that the dactylo**sco**pic data stored in SIS belong to the person. Member States shall communicate **information about the identity and the whereabouts of the person through the exchange of** supplementary information in order to facilitate timely investigation of the case.
517			**CHAPTER XIa**	**CHAPTER XIa**
518			**SPECIFIC RULES FOR BIOMETRIC DATA**	**SPECIFIC RULES FOR BIOMETRIC DATA**
519			*Article **41A (ex-Article** 22**)***	*Article **41A (ex-Article** 22**)***
520			*Specific rules for entering photographs, facial images,*	*Specific rules for entering photographs, facial images,*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			*dactylo~~graphic~~**scopic** data and DNA profiles*	*dactylo~~graphic~~**scopic** data and DNA profiles*
521			1. The entering into SIS of data referred to in Article 20(3)(w), (x) and (y) shall be subject to the following provisions:	LIBE proposal: 1. ***Only facial images and dactyloscopic data*** referred to in Article 20(2)(w) and (x) ***which fulfil a minimum data quality standard*** shall ~~only~~ be entered into SIS***. Before such data are entered,*** ~~following~~ a quality check ***shall be performed in order*** to ascertain ***whether*** ~~a~~ ***the*** ~~fulfilment of a~~ minimum data quality standard ***has been met***.
522				*Informal outcome of technical discussion* ***1a. Dactyloscopic data entered in SIS shall consist of one to ten flat fingerprints or one to ten rolled fingerprints [and may consist of [two] palm prints [if available]].***
523			(a) Photographs, facial images, dactylo~~graphic~~**scopic** data and DNA profiles shall only be entered following a quality check to ascertain the fulfilment of a minimum data quality standard.	***Deletion (moved under para. 1)***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
524			(b) A DNA profile may only be added to alerts provided for in Article 32(2)(a) and (c) and only where photographs, facial images or dactylo~~graphic~~**scopic** data suitable for identification are not available **or not sufficient**. The DNA profiles of persons who are direct ascendants, descendants or siblings of the alert subject may be added to the alert provided that those persons concerned give~~s~~ explicit consent. ~~The racial origin of the person shall not be included in the DNA profile.~~	LIBE proposal: ***1b.*** A DNA profile may only be added to alerts ***in the situations*** provided for in ***Article 32***(2)(a) ***only following a quality check to ascertain whether the*** minimum data quality standard ***has been met*** and only where photographs, facial images or ***dactyloscopic*** data suitable for identification are not available. The DNA profiles of persons who are direct ascendants, descendants or siblings of the alert subject may be added to the alert provided that those persons concerned give explicit consent. ***Where a DNA profile is added to an alert, that profile shall contain the minimum information strictly necessary for the identification of the missing person and, in all event, shall always exclude the racial origin and health information about that person***.
525			2. Quality standards shall be established for the storage of the data referred to under paragraph 1(a) of this Article and Article 40. The specification of these standards shall be laid down by means of	LIBE proposal: 2. Quality standard~~s~~ shall be established for the storage of ***the biometric*** data referred to in paragraph 1. ***These quality standards shall set the level of***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			implementing measures and updated in accordance with the examination procedure referred to in Article 72(2).	***quality required for using the data to verify the identity of a person in accordance with Article 42 (1) and for using the data to identify a person in accordance with Article 42 (2)-(4).***
526				LIBE proposal: ***2a.*** The ***quality*** ~~specification of these~~ standards ***referred to in paragraphs 1, 1b and 2*** shall be laid down by means of implementing measures and updated in accordance with the examination procedure referred to in Article 72(2).
527	*Article 42*	*Article 42*	*Article 42*	*Article 42*
528	*Specific rules for verification or search with photographs, facial images, dactylographic data and DNA profiles*	*Specific rules for verification or search with photographs, facial images, **dactyloscopic** data and DNA profiles*	*Specific rules for verification or search with photographs, facial images, dactylo**sco**~~graph~~ic data and DNA profiles*	*Specific rules for verification or search with photographs, facial images, dactylo**sco**~~graph~~ic data and DNA profiles*
529	1. Photographs, facial images, dactylographic data and DNA profiles shall be retrieved from SIS to verify the identity of a person who has been located as a result of an alphanumeric search made in SIS.	1. ***Where photographs***, facial images, ***dactyloscopic*** data and DNA profiles ***are contained within an alert in SIS, such data*** shall be retrieved from SIS to ***confirm*** the identity of a person who has been ***found*** as a result of an alphanumeric search made in SIS.	1. Photographs, facial images, dactylo**sco**~~graph~~ic data and DNA profiles shall be retrieved, **whenever it is necessary,** from SIS to verify the identity of a person who has been located as a result of an alphanumeric search made in SIS.	***1. Where photographs,*** facial images and dactyloscopic data ***are available in an alert in*** SIS, ***such data*** shall be ***used*** to ***confirm*** the identity of a person who has been located as a result of an alphanumeric search made in SIS.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
530		***1a. To check whether the person already appears in SIS under another identity, a fingerprint search may be carried out before a new alert is issued***.		As part of an overall compromise with Art. 23a, could be withdrawn.
531	2. Dactylographic data may also be used to identify a person. Dactylographic data stored in SIS shall be searched for identification purposes if the identity of the person cannot be ascertained by other means.	2. ***Dactyloscopic*** data may also be used to identify a person. ***Dactyloscopic*** data stored in SIS shall be ***used*** for identification purposes ***only*** if the identity of the person cannot be ascertained by ***alphanumeric data***. ***For this purpose the Central SIS shall contain an automated fingerprint identification system (AFIS).***	2. ~~Dactylographic data stored in SIS shall be searched for identification purposes i~~**I**f the identity of the person cannot be ascertained by other means **dactyloscopic data shall be** ~~used~~ **searched for identification purposes**. Dactylo**sco**~~graph~~hic data may ~~also~~ be ~~used~~ **searched in all cases** to identify a person.	LIBE proposal (to combine the Council and EP position): **I**f the identity of the person cannot be ascertained by other means**, dactyloscopic data shall be searched for identification purposes. Dactyloscopic data may be searched in all cases to identify a person**. ***For this purpose the Central SIS shall contain an Automated Fingerprint Identification System (AFIS)***. Council to check.
532		***2a. Member States shall make available to end-users an Automated Fingerprint Identification System at the latest two years after the entry into force of this Regulation. They shall take necessary measures to that end, including, where necessary, adjustments to their N.SIS.***		To be further discussed, especially whether defining a date in the Regulation is indeed the right approach. Commission services proposal: ***Within two years following the entry into force of this Regulation, Member States shall enable end-users to conduct searches with dactyloscopic data.***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				[Linked to Art. 58] LIBE does agree with this COM proposal, provided that "automated" is inserted before "searches"
533	3. Dactylographic data stored in SIS in relation to alerts issued pursuant to Articles 26, 34(1) b) and d) and Article 36 may also be searched by using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of crimes under investigation, and where it can be established to a high degree of probability that they belong to the perpetrator of the offence provided that the competent authorities are unable to establish the identity of the person by using any other national, European or international database.	3. ***Dactyloscopic*** data stored in SIS in relation to alerts issued pursuant to Articles 26, 34(1) b) and d) and Article 36 may also be searched by using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of ***terrorist offences or other serious*** under investigation, and where it can be established to a high degree of probability that they belong to the perpetrator of the ***terrorist*** offence ***or other serious crime*** provided that the competent authorities are unable to establish the identity of the person by using any other national, European or international database.	3. Dactyloscog~~raph~~ic data stored in SIS in relation to alerts issued pursuant to Articles 26, **32,** 34~~(1) b) and d)~~**, 36** and ~~Article 36~~ **40** may also be searched by using complete or incomplete sets of fingerprints or palm prints discovered at the scenes of **serious** crimes **or terrorist offences**[129] under investigation, and where it can be established to a high degree of probability that they belong to ~~the~~ **a** perpetrator of the offence ~~provided that the competent authorities are unable to establish the identity of the person by using any other national, European or international database~~.	The EP will come back on this point later in particular on the Council's deletion
534		***3a. Where final identification in accordance with this Article reveals that the result of the comparison received from the Central SIS does not correspond to the dactyloscopic data sent for***		LIBE will come back on this point

[129] In line with Article 40.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		comparison, Member States shall immediately erase the result of the comparison and communicate this to the Agency as soon as possible and no later than within three working day.		
535	4. As soon as this becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person. Identification based on photographs or facial images shall only be used at regular border crossing points where self-service systems and automated border control systems are in use.	4. ***The Commission is empowered to adopt a delegated act in accordance with Article 71a determining the use of photographs and facial images and DNA profiles for the purpose of identifying persons and the technical standards for doing so including the search, as well as the identification and confirmation of identity. The Commission shall adopt that delegated act as*** soon as this becomes technically possible ***with*** a high degree of reliability of identification, photographs and facial images may be used to identify a person. Identification based on photographs or facial images shall only be used at regular border crossing points where self-service systems and automated border control systems	4. As soon as this becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person. **Before the functionality is implemented, the Commission shall present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted.**[130] Identification based on photographs or facial images shall ~~only~~ be used **subject to national law** ~~at regular border crossing points where self-service systems and automated border control systems are in use~~.	LIBE proposal: 4. ***Facial images may be used to identify a person/third country national*** ~~As~~ ***as*** soon as this becomes technically possible ~~and~~ ***with*** ~~and while ensuring~~ a high degree of reliability ~~of identification, photographs and facial images may be used to identify a person~~. ***Before that functionality is implemented, the Commission shall present a report on the availability, and readiness and reliabilty of the required technology, on which the European Parliament shall be consulted.*** Identification based on photographs or facial images shall only be used in the context of regular border crossing points where self-service systems and automated border control systems are in use. ***X years***

[130] Similar to the text of Article 22(c) of Regulation (EC) No 1987/2006 of 20 December on the establishment, operation and use of the second generation Schengen Information System (SIS II).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		are in use.		***after the start of the use of the functionality at such regular border crossing points, the Commission is empowered to adopt delegated acts in accordance with Article 54a concerning the determination of other circumstances in which photographs and facial images may be used for the identification of persons/ third-country nationals.*** Commission services proposal: 4. As soon as this becomes technically possible, and while ensuring a high degree of reliability of identification, photographs and facial images may be used to identify a person. Identification based on photographs or facial images shall only be used in the context of regular border crossing points where self-service systems and automated border control systems are in use. **Before this functionality is implemented in SIS, the Commission shall present a report on the availability and readiness of the required**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				technology, on which the European Parliament shall be consulted.[131] ***Following the deployment at border cross points, t****he Commission **shall be** empower**ed** to adopt a delegated act in accordance with Article 54a determining in which other circumstances facial images can be used for the identification of third-country nationals .* Council can accept adding the reference to reliability to the Commission services proposal as a compromise. Political agreement was reached during trilogue on 07-02-2018. To be fine-tuned at technical level (on the basis of COM Services proposal).
536	**CHAPTER XII**	**CHAPTER XII**	**CHAPTER XII**	
537	**RIGHT TO ACCESS AND RETENTION OF ALERTS**	**RIGHT TO ACCESS AND RETENTION OF ALERTS**	**RIGHT TO ACCESS AND RETENTION OF ALERTS**	
538	*Article 43*	*Article 43*	*Article 43*	*Article 43*

[131] Similar to the text of Article 22(c) of Regulation (EC) No 1987/2006 of 20 December on the establishment, operation and use of the second generation Schengen Information System (SIS II).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
539	*Authorities having a right to access alerts*	*Authorities having a right to access alerts*	*Authorities having a right to access alerts*	Entire Article to be further discussed
540	1. Access to data entered in SIS and the right to search such data directly or in a copy of SIS data shall be reserved to the authorities responsible for:		1. **National competent authorities shall have** ~~A~~**a**ccess to data entered in SIS and the right to search such data directly or in a copy of SIS data ~~shall be reserved to the authorities responsible~~ for **the purposes of**:	
541	(a) border control, in accordance with 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 (Schengen Borders Code);		(a) border control, in accordance with 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 (Schengen Borders Code);	(a) border control, in accordance with 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 (Schengen Borders Code);
542	(b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities;		(b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities;	(b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities;
543	(c) other law enforcement activities carried out for the prevention, detection and investigation of criminal	(c) the prevention, detection and investigation of ***terrorist offences or other serious*** criminal offences within the Member State	(c) other ~~law enforcement~~ activities carried out for the prevention, detection**,** ~~and~~ investigation **or prosecution**	LIBE proposal (based on Article 1(1) of Directive 2016/680

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	offences within the Member State concerned;	concerned ***and to which Directive (EU) 2016/680 applies***;	of criminal offences **or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public or national security** within the Member State concerned;[59]	(c) the prevention, detection**,** ~~and~~ investigation **or prosecution** of ~~***terrorist offences or other serious***~~ criminal offences **or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public ~~or national~~ security** within the Member State concerned ***and to which Directive (EU) 2016/680 applies***; **COM services proposal of 23 January:** (c) the prevention, detection**,** and investigation **or prosecution** of ***terrorist offences or other serious*** criminal offences **or the execution of criminal penalties, ~~including the safeguarding against and the prevention of threats to public or national security~~** within the Member State concerned ***and to which Directive (EU) 2016/680 applies***; LIBE does not agree with this COM proposal
544	(d) examining the conditions and taking decisions related to		(d) examining the conditions and taking decisions related to	(d) examining the conditions and taking decisions related to the entry and stay of third-

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals.		the entry and stay of third-country nationals on the territory of the Member States, ~~including~~ on residence permits**,** ~~and~~ long-stay visas, and to the return of third-country nationals.	country nationals on the territory of the Member States, ~~including~~ on residence permits**,** ~~and~~ long-stay visas, and to the return of third-country nationals;
545		***(da) security checks in the context of procedures related to applications for international protection, insofar as those authorities do not constitute "determining authorities" as defined in Article 2(f) of Directive 2013/32/EU of the European Parliament and of the Council[132], and where relevant providing advice in accordance with Council Regulation(EU) 377/2004[133].***		LIBE proposal merging (da) of Parliament and (f) of Council: To be checked. ***(da) security checks on third-country nationals in the context of procedures related to applications for international protection, insofar as those authorities do not constitute "determining authorities" as defined in Article 2(f) of Directive 2013/32/EU of the European Parliament and of the Council[134], and where relevant providing advice in accordance with Council***

[132] ***Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).***

[133] ***Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network (OJ L 64, 2.3.2004, p. 1).***

[134] ***Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				Regulation(EU) 377/2004[135];
546	(e) checks on third-country nationals who are illegaly entering or staying on the territory of the Member States as well as on applicants for international protection;		(e) checks on third-country nationals who are illegaly entering or staying on the territory of the Member States as well as on applicants for international protection;	(e) checks on third-country nationals who are illegaly entering or staying on the territory of the Member States as well as on applicants for international protection;
547			**1a. The right to access data entered in SIS and the right to search such data directly may be exercised by national competent authorities responsible for naturalization, in the performance of their tasks, as provided for in national law, and by their coordinating authorities.**	See under (da) To be checked.
548	2. The right to access data entered in SIS and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial		2. The right to access data entered in SIS and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial	Will come back on this paragraph 2. The right to access data entered in SIS and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial

[135] ***Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network (OJ L 64, 2.3.2004, p. 1).***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	inquiries prior to charge, in the performance of their tasks, as provided for in national law, and by their coordinating authorities.		inquiries prior to charge, in the performance of their tasks, as provided for in national law, and by their coordinating authorities.	inquiries prior to charge, in the performance of their tasks, as provided for in national law, and by their coordinating authorities.
549	3. The right to access data entered in SIS and to search such data directly may be exercised by the authorities competent to carry out the tasks referred to in paragraph 1(c) in the performance of these tasks. The access by these authorities shall be governed by the law of each Member State.	3. The right to access data entered in SIS and to search such data directly may be exercised by the authorities referred to in paragraph 1(c) in the performance of these tasks. The access by these authorities shall be ***in accordance with this Regulation and with Union law on data protection.***	3. The right to access data entered in SIS and to search such data directly may be exercised by the authorities competent to carry out the tasks referred to in paragraph 1(c) in the performance of these tasks. The access by these authorities shall be governed by the **national** law ~~of each Member State~~.	Will come back on this paragraph
550	4. The authorities referred to in this Article shall be included in the list referred to in Article 53(8).		4. The authorities referred to in this Article shall be included in the list referred to in Article 53(8).	4. The authorities referred to in this Article shall be included in the list referred to in Article 53(8).
551	*Article 44*	*Article 44*	*Article 44*	*Article 44*
552	*Vehicle registration authorities*	*Vehicle registration authorities*	*Vehicle registration authorities*	*Vehicle registration authorities*
553	1. The services in the Member States responsible for issuing registration certificates for vehicles, as referred to in Council Directive 1999/37/EC[136], shall	1. The ***competent authorities*** in the Member States responsible for issuing registration certificates for vehicles, as referred to in Council Directive 1999/37/EC[137],	1. The services in the Member States responsible for issuing registration certificates for vehicles, as referred to in Council	Presidency proposal 1. The services in the Member States responsible for issuing registration certificates for

[136] Council Directive 1999/37 of 29 April 1999 on the registration of documents for vehicles (OJ L 138, 1.6.1999, p. 57).
[137] Council Directive 1999/37 of 29 April 1999 on the registration of documents for vehicles (OJ L 138, 1.6.1999, p. 57).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	have access to the following data entered into SIS in accordance with Article 38(2)(a), (b), (c) and (l) of this Regulation for the sole purpose of checking whether vehicles presented to them for registration have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:	shall have access ***only*** to the following data entered into SIS in accordance with Article 38(2)(a), (b), (c) and (l) of this Regulation for the sole purpose of checking whether vehicles presented to them for registration have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:	Directive 1999/37/EC[138], shall have access to ~~the following~~ data entered into SIS in accordance with Article 38(2)(a), (b), (c)**,** ~~and~~ (l) **and (o)** of this Regulation for the sole purpose of checking whether **motor** vehicles **and accompanying vehicle registration certificates and vehicle number plates** presented to them for registration have been stolen, misappropriated or lost **or purport to be such a document but are false** or are sought as evidence in criminal proceedings~~:~~**.**	vehicles, as referred to in Council Directive 1999/37/EC[139], shall have access to ~~the following~~ data entered into SIS in accordance with Article 38(2)(a), (b), (c)**,** ~~and~~ (l) **and (o)** of this Regulation for the sole purpose of checking whether **motor** vehicles **and accompanying vehicle registration certificates and vehicle number plates** presented to them for registration have been stolen, misappropriated or lost **or purport to be such a document but are false** or are sought as evidence in criminal proceedings~~:~~**.**
554	(a) data on motor vehicles, as defined by national law, regardless of the propulsion system;		~~(a) data on motor vehicles, as defined by national law, regardless of the propulsion system;~~	**Deleted**
555	(b) data on trailers with an unladen weight exceeding 750 kg and caravans;		~~(b) data on trailers with an unladen weight exceeding 750 kg and caravans;~~	**Deleted**
556	(c) data concerning vehicle registration certificates and vehicle number plates which have been stolen,		~~(c) data concerning vehicle registration certificates and vehicle number plates which have been stolen,~~	**Deleted**

138 Council Directive 1999/37 of 29 April 1999 on the registration of documents for vehicles (OJ L 138, 1.6.1999, p. 57).
139 Council Directive 1999/37 of 29 April 1999 on the registration of documents for vehicles (OJ L 138, 1.6.1999, p. 57).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	misappropriated, lost or invalidated.		~~misappropriated, lost or invalidated.~~	
557	Access to those data by the services responsible for issuing registration certificates for vehicles shall be governed by the national law of that Member State.	Access to those data by the ***competent authorities referred to in the first subparagraph*** shall be governed by the national law of ***the*** Member State ***of the competent authority in question***.	Access to those data by the services responsible for issuing registration certificates for vehicles shall be governed by the national law of that Member State.	Presidency proposal Access to those data by the services responsible for issuing registration certificates for vehicles shall be governed by the national law of that Member State.
558	2. Services as referred to in paragraph 1 that are government services shall have the right to access directly the data entered in SIS.	***deleted***	2. Services as referred to in paragraph 1 that are government services shall have the right to access directly the data entered in SIS.	Presidency proposal 2. Services as referred to in paragraph 1 that are government services shall have the right to access directly the data entered in SIS.
559	3. Services as referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access those data directly and to pass them on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect	***deleted***	3. Services as referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access those data directly and to pass them on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect	Presidency proposal 3. Services as referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access those data directly and to pass them on to the service concerned. The Member State concerned shall ensure that the service in question and its

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	any limitations on the permissible use of data passed on to them by the authority.		any limitations on the permissible use of data passed on to them by the authority.	employees are required to respect any limitations on the permissible use of data passed on to them by the authority.
560	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS which gives rise to suspicion of the commission of a criminal offence shall be governed by national law.	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by ***competent authorities*** as referred to in paragraph 1 of any information ***obtained*** by access to SIS which gives rise to suspicion of the commission of a criminal offence shall be governed by national law.	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS ~~which gives rise to suspicion of the commission of a criminal offence~~ shall be governed by national law.	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information **obtained** by access to SIS shall be governed by national law.
561	*Article 45*	*Article 45*	*Article 45*	*Article 45*
562	*Registration authorities for boats and aircraft*	*Registration authorities for boats and aircraft*	*Registration authorities for boats and aircraft*	*Registration authorities for boats and aircraft*
563	1. The services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines and aircraft shall have access to the following data entered into SIS in accordance with Article 38(2) of this Regulation for the sole purpose of checking whether boats, including	1. The ***competent authorities*** in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines and aircraft shall have access ***only*** to the following data entered into SIS in accordance with Article 38(2) of this Regulation for the sole purpose of checking whether boats,	1. The services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines and aircraft shall have access to the following data entered into SIS in accordance with Article 38(2) of this Regulation for the sole purpose of checking whether boats, including	Presidency proposal 1. The services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines and aircraft shall have access to the following data entered into SIS in accordance with Article 38(2) of this

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	boat engines; aircraft or containers presented to them for registration or subject of traffic management have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:	including boat engines; aircraft or containers presented to them for registration or subject of traffic management have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:	boat engines~~;~~**,** aircraft**, including aircraft engines** ~~or containers~~ presented to them for registration or subject of traffic management have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:	Regulation for the sole purpose of checking whether boats, including boat engines~~;~~**,** aircraft**, including aircraft engines** presented to them for registration or subject of traffic management have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings:
564	(a) data on boats;		(a) data on boats;	(a) data on boats;
565	(b) data on boat engines;		(b) data on boat engines;	(b) data on boat engines;
566	(c) data on aircraft.	***(ca) data on aircraft engines.***	(c) data on aircraft**;**	(c) data on aircraft**;**
567			**(d) data on aircraft engines**.	**(d) data on aircraft engines**.
568	Subject to paragraph 2, the law of each Member State shall govern access to those data by those services in that Member State. Access to the data listed (a) to (c) above shall be limited to the specific competence of the services concerned.	***Access*** to those data by ***the competent authorities referred to in the first subparagraph shall be governed by the national law of the*** Member State ***of the competent authority in question***. Access to the data listed ***in points (a), (b) (c) and (ca) of the first subparagraph*** shall be limited to the specific competence of the ***competent authorities*** concerned.	Subject to paragraph 2, the law of each Member State shall govern access to those data by those services in that Member State. Access to the data listed (a) to (**d**~~c~~) above shall be limited to the specific competence of the services concerned.	Presidency proposal Subject to paragraph 2, the law of each Member State shall govern access to those data by those services in that Member State. Access to the data listed (a) to (**d**~~c~~) above shall be limited to the specific competence of the services concerned.
569	2. Services as referred to in paragraph 1 that are government services shall have the right to	***deleted***	2. Services as referred to in paragraph 1 that are government services shall have the right to	Presidency proposal 2. Services as referred to in paragraph 1 that are government

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	access directly the data entered in SIS.		access directly the data entered in SIS.	services shall have the right to access directly the data entered in SIS.
570	3. Services referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access the data directly and to pass those data on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations on the permissible use of data conveyed to them by the authority.	***deleted***	3. Services referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access the data directly and to pass those data on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations on the permissible use of data conveyed to them by the authority.	Presidency proposal 3. Services referred to in paragraph 1 that are non-government services shall have access to data entered in SIS only through the intermediary of an authority as referred to in Article 43 of this Regulation. That authority shall have the right to access the data directly and to pass those data on to the service concerned. The Member State concerned shall ensure that the service in question and its employees are required to respect any limitations on the permissible use of data conveyed to them by the authority.
571	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS which gives rise to suspicion of a criminal	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by ***competent authorities*** as referred to in paragraph 1 of any information ***obtained*** by access to SIS which gives rise to suspicion	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS which gives rise to suspicion of a criminal	4. Article 39 of this Regulation shall not apply to access gained in accordance with this Article. The communication to the police or judicial authorities by services as referred to in paragraph 1 of any information ***obtained*** by

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	offence shall be governed by national law.	of a criminal offence shall be governed by national law.	offence shall be governed by national law.	access to SIS e shall be governed by national law.
572			***Article 45A***	***Article 45A*** Presidency proposal for the whole Article
573			***Registration authorities for firearms***	***Registration authorities for firearms***
574			**1. The services in the Member States responsible for issuing registration certificates for firearms, shall have access to data on persons subject to an alert under Article 26 or 36 and firearms entered into SIS in accordance with Article 38(2) of this Regulation for the purpose of checking whether the person requesting registration represents a threat to public or national security or whether firearms presented to them for registration are sought for seizure or for use as evidence in criminal proceedings.**	**1. The services in the Member States responsible for issuing registration certificates for firearms, shall have access to data on persons subject to an alert under Article 26 or 36 and firearms entered into SIS in accordance with Article 38(2) of this Regulation for the purpose of checking whether the person requesting registration represents a threat to public or national security or whether firearms presented to them for registration are sought for seizure or for use as evidence in criminal proceedings.**
575			**2. Access to those data by those services shall be governed by the national law of that**	**2. Access to those data by those services shall be governed by the national law of that Member**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			Member State.[140] Access to those data shall be limited to the specific competence of the services concerned.	**State.[141] Access to those data shall be limited to the specific competence of the services concerned.**
576			**3. Services as referred to in paragraph 1 that are competent authorities may have the right to access directly the data entered in SIS.**	**3. Services as referred to in paragraph 1 that are competent authorities may have the right to access directly the data entered in SIS.**
577			**4. Services as referred to in paragraph 1 that are not competent authorities shall have access to data entered in SIS through intermediation by an authority referred to in Article 43 of this Regulation. The intermediating authority shall have the right to access the data directly and shall inform the service concerned if the firearm can be registered or not. The Member State shall ensure that the service in question and its employees are required to respect any limitations o the permissible use of data conveyed**	**4. Services as referred to in paragraph 1 that are not competent authorities shall have access to data entered in SIS through intermediation by an authority referred to in Article 43 of this Regulation. The intermediating authority shall have the right to access the data directly and shall inform the service concerned if the firearm can be registered or not. The Member State shall ensure that the service in question and its employees are required to respect any limitations o the permissible use of data conveyed**

140 Wording in line with Article 44(1), last subparagraph.
141 Wording in line with Article 44(1), last subparagraph.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			to them by the intermediating authority.	**to them by the intermediating authority.**
578			**5. Article 39 shall not apply to access gained in accordance with this Article. The communication to the police or the judicial authorities by services as referred to in paragraph 1 of any information brought to light by access to SIS shall be governed by national law.**	**5. Article 39 shall not apply to access gained in accordance with this Article. The communication to the police or the judicial authorities by services as referred to in paragraph 1 of any information *obtained* by access to SIS shall be governed by national law.**
579	*Article 46*	*Article 46*	*Article 46*	*Article 46*
580	*Access to SIS data by Europol*	*Access to SIS data by Europol*	*Access to SIS data by Europol*	*Access to SIS data by Europol*
581	1. The European Union Agency for Law Enforcement Cooperation (Europol) shall have, within its mandate, the right to access and search data entered into SIS.	1. The European Union Agency for Law Enforcement Cooperation (Europol) shall***, where necessary to fulfill*** its mandate***, have*** the right to access and search data entered into SIS.	1. The European Union Agency for Law Enforcement Cooperation (Europol) shall have, within its mandate, the right to access and search data entered into SIS **and may exchange and process supplementary information in accordance with the provisions of the SIRENE Manual laid down in Article 8**.	Outcome of drafting meeting of 13 April: 1. The European Union Agency for Law Enforcement Cooperation (Europol) shall***, where necessary to fulfil*** its mandate, have the right to access and search data entered into SIS **and may exchange *and further request* ~~process~~ supplementary information in accordance with the provisions of the SIRENE Manual laid down in Article 8**.
582	2. Where a search by Europol reveals the existence of an alert in	2. Where a search by Europol reveals the existence of an alert in SIS, Europol shall ***immediately***	2. Where a search by Europol reveals the existence of an alert in	**COM services proposal of 23 January:**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	SIS, Europol shall inform the issuing Member State via the channels defined by Regulation (EU) 2016/794.	inform the issuing Member State ***through the exchange of supplementary information by means of the communication infrastructure and in accordance with the provisions set out in the SIRENE Manual. Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States*** via the channels defined by Regulation (EU) 2016/794.	SIS, Europol shall inform the issuing Member State via the **exchange of supplementary information. Until the time that Europol has implemented the functionality to exchange supplementary information, it shall inform the issuing Member State via the** channels defined by Regulation (EU) 2016/794.	(2) Where a search by Europol reveals the existence of an alert in SIS, Europol shall ~~***immediately***~~ inform the issuing Member State ***through the exchange of supplementary information by means of the communication infrastructure and in accordance with the provisions set out in the SIRENE Manual. [Until Europol is able to use the functionalities intended for the exchange of supplementary information, it shall inform issuing Member States*** via the channels defined by Regulation. (EU) 2016/794.] LIBE does agree with this COM proposal Last sentence in bracket is subject to the outcome of the discussion on the entry into operation.
583			**2a. Europol may process the supplementary information that has been provided to it by Member States for the purposes of cross-checking, aimed at identifying connections or other relevant links and for strategic, thematic and operational analyses as defined in points (a) and (c) of Article 18(2) of Regulation (EU) 2016/794 . Any processing by Europol of**	Outcome of drafting meeting of 13 April: **2a. Europol may process the supplementary information that has been provided to it by Member States for the purposes of *comparing with its databases and analytical files* ~~cross-checking~~, aimed at identifying connections or other relevant links and for strategic, thematic or operational analyses as defined in points (a), (b) and (c) of Article 18(2) of Regulation (EU) 2016/794 .**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			supplementary information shall be carried out in accordance with Regulation (EU) 2016/794.	**Any processing by Europol of supplementary information *for the purposes indicated in this paragraph*, shall be carried out in accordance with Regulation (EU) 2016/794.** The EP to confirm.
584	3. The use of information obtained from a search in the SIS is subject to the consent of the Member State concerned. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the Member State concerned.	3. The use of information obtained from a search in the SIS is subject to the consent of the ***issuing*** Member State. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the ***issuing*** Member State ***and in full respect of Union law on data protection***.	3. The use of information obtained from a search in ~~the~~ SIS **or from the processing of supplementary information** is subject to the consent of the **issuing** Member State ~~concerned~~. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the **issuing** Member State ~~concerned~~.	3. The use of information obtained from a search in ~~the~~ SIS **or from the processing of supplementary information** is subject to the consent of the **issuing** Member State. If the Member State allows the use of such information, the handling thereof by Europol shall be governed by Regulation (EU) 2016/794. Europol may only communicate such information to third countries and third bodies with the consent of the **issuing** Member State ***and in full respect of Union law on data protection.***
585	4. Europol may request further information from the Member State concerned in accordance with the provisions of Regulation (EU) 2016/794.	4. Europol may request further information from the ***issuing*** Member State in accordance with the provisions of Regulation (EU) 2016/794.	4. ~~Europol may request further information from the Member State concerned in accordance with the provisions of Regulation (EU) 2016/794.~~ [142]	Outcome of drafting meeting of 13 April: (deleted)

[142] In accordance with Regulation 2016/794, Europol may in any event request information related to mandated offences from the Member States. Paragraph 4 may therefore be considered superfluous.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
586	5. Europol shall:		5. Europol shall:	5. Europol shall:
587	(a) without prejudice to paragraphs 3, 4 and 6, not connect parts of SIS nor transfer the data contained therein to which it has access to any computer system for data collection and processing operated by or at Europol nor download or otherwise copy any part of SIS;		(a) without prejudice to paragraphs 3~~, 4~~ and 6, not connect parts of SIS nor transfer the data contained therein to which it has access to any computer system for data collection and processing operated by or at Europol nor download or otherwise copy any part of SIS;	(a) without prejudice to paragraphs 3~~, 4~~ and 6, not connect parts of SIS nor transfer the data contained therein to which it has access to any computer system for data collection and processing operated by or at Europol nor download or otherwise copy any part of SIS;
588			**(aa) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted from SIS, unless the continued storage of the data is deemed necessary, on the basis of information that is more extensive than that possessed by the data provider, in order for Europol to perform its tasks. Europol shall inform the data provider of the continued storage of such**	**COM services proposal of 23 January:** **(aa) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted from SIS~~,~~. If Europol has information in its databases or analytical files on a case to which the supplementary information is related, ~~unless~~ in order for Europol to perform its tasks, the continued storage of the ~~data~~ supplementary information ~~is~~ may be deemed necessary, ~~on the basis of information that is more extensive than that possessed by the data~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			data and present a justification of such continued storage;	**~~provider. ,~~. Europol shall inform the ~~data provider~~ the issuing and the executing Member State of the continued storage of such ~~data~~ supplementary information and present a justification of such continued storage;** LIBE proposal: **(aa) notwithstanding Article 31(1) of Regulation (EU) 2016/794, delete supplementary information containing personal data at the latest one year after the related alert has been deleted from SIS~~,~~;**
a.	(b) limit access to data entered in SIS to specifically authorised staff of Europol;	(b) limit access to data entered in SIS to specifically authorised staff of Europol ***requiring access for the performance of their tasks***;	(b) limit access to data entered in SIS**, including supplementary information,** to specifically authorised staff of Europol;	(b) limit access to data entered in SIS**, including supplementary information** to specifically authorised staff of Europol ***requiring access for the performance of their tasks***;
b.	(c) adopt and apply measures provided for in Articles 10 and 11;	(c) adopt and apply measures provided for in Articles 10**,** 11, ***13 and 14***;	(c) adopt and apply measures provided for in Articles 10 and 11; **and**	Revised LIBE proposal, outcome of drafting meeting of 13 April: (c) adopt and apply ~~***take***~~ measures ***to ensure security, ~~and~~ confidentiality and self-monitoring as provided for in Articles*** **10, ~~and~~ 11 ~~,~~ *~~and 13 and 14(1) apply mutatis mutandis;~~ and***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
c.				(cc) ***ensure that its staff authorized to process SIS data receives appropriate training and information in accordance with Article 14(1).***
d.	(d) allow the European Data Protection Supervisor to review the activities of Europol in the exercise of its right to access and search data entered in SIS.		(d) allow the European Data Protection Supervisor to review the activities of Europol in the exercise of its right to access and search data entered in SIS **and the exchange and processing of supplementary information**.	(d) allow the European Data Protection Supervisor to monitor and review the activities of Europol in the exercise of its right to access and search data entered in SIS **and the exchange and processing of supplementary information**.
e.				LIBE proposal: **5a. Without prejudice to paragraph 5(aa), Europol may store supplementary information containing personal data beyond the period in point (aa) if it has information in its databases or analytical files on a case to which the supplementary information is related and such continued storage is strictly necessary in order for Europol to perform its tasks. In such cases, Europol shall inform the ~~data provider~~ issuing and the executing Member State of the continued storage of the**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				~~data~~ **supplementary information and provide a justification for the continued storage.**
589	6. Data may only be copied for technical purposes, provided that such copying is necessary in order for duly authorised Europol staff to carry out a direct search. The provisions of this Regulation shall apply to such copies. The technical copy shall be used for the purpose of storing SIS data whilst those data are searched. Once the data have been searched they shall be deleted. Such uses shall not be construed to be an unlawful downloading or copying of SIS data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS into other Europol systems.		6. Data may only be copied for technical purposes, provided that such copying is necessary in order for duly authorised Europol staff to carry out a direct search. The provisions of this Regulation shall apply to such copies. The technical copy shall be used for the purpose of storing SIS data whilst those data are searched. Once the data have been searched they shall be deleted. Such uses shall not be construed to be an unlawful downloading or copying of SIS data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS into other Europol systems.	6. Data may only be copied for technical purposes, provided that such copying is necessary in order for duly authorised Europol staff to carry out a direct search. The provisions of this Regulation shall apply to such copies. The technical copy shall be used for the purpose of storing SIS data whilst those data are searched. Once the data have been searched they shall be deleted. Such uses shall not be construed to be an unlawful downloading or copying of SIS data. Europol shall not copy alert data or additional data issued by Member States or from CS-SIS into other Europol systems.
590	7. Any copies, as referred to in paragraph 6, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in an emergency until the emergency comes to an end. Europol shall report any such extensions to the	7. Any copies, as referred to in paragraph 6, which lead to off-line databases may be retained for a period not exceeding 48 hours. ***Where Europol creates an offline database with SIS data, it*** shall report ***the existence of*** such ***a database*** to the European Data Protection Supervisor.	7. ~~Any copies, as referred to in paragraph 6, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in an emergency until the emergency comes to an end. Europol shall report any such extensions to the~~	(deleted)

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	European Data Protection Supervisor.		~~European Data Protection Supervisor.~~	
591	8. Europol may receive and process supplementary information on corresponding SIS alerts provided that the data processing rules referred to in paragraphs 2 to 7 are applied as appropriate.		8. ~~Europol may receive and process supplementary information on corresponding SIS alerts provided that the data processing rules referred to in paragraphs 2~~**5** ~~to 7 are applied as appropriate.~~	(deleted)
592	9. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity Europol should keep log of every access to and search in SIS. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.	9. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity Europol ***shall*** keep logs of every access to and search in SIS. ***Such logs shall show, in particular, the date and time of the data processing activity, the type of data processed and the name of the persone responsible for processing the data.*** Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS. ***The content, retention period and rules and formats for the logs are defined in accordance with Article 12.***	9. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity Europol ~~should~~ **shall** keep log**s** of every access to and search in SIS **in accordance with Article 12**. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.	LIBE proposal: 9. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity Europol sh**all**~~ould~~ keep logs of every access to and search in SIS **in accordance with the provisions of Article 12**. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.
593		***9a. Europol shall be immediately informed by Member States of any alerts created under***		**COM services proposal of 23 Jan 2018:**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		Articles 34, 36 or 38 and hits concerning those alerts where a person or an object is sought by a Member State in relation to an offence referred to in Directive (EU) 2017/541.		***9a. Europol shall be ~~immediately~~ informed by Member States of any alerts created under Article 24 and hits concerning those alerts where a person is sought by a Member State in relation to ~~an~~ a terrorist offence ~~referred to in Directive (EU) 2017/541.~~*** LIBE does agree with this COM proposal
594	*Article 47*	*Article 47*	*Article 47*	*Article 47*
595	*Access to SIS data by Eurojust*	*Access to SIS data by Eurojust*	*Access to SIS data by Eurojust*	*Access to SIS data by Eurojust*
596	1. The national members of Eurojust and their assistants shall, within their mandate, have the right to access and search data entered in SIS within their mandate, in accordance with Articles 26, 32, 34 38 and 40.	1. ***Only the*** national members of Eurojust and their assistants shall, ***where necessary to execute their duties and*** within their mandate, have the right to access and search data entered in SIS within their mandate, in accordance with Articles 26, 32, 34**,** 38 and 40.	1. The national members of Eurojust and their assistants shall, within their mandate, have the right to access and search data entered in SIS within their mandate, in accordance with Articles 26, 32, 34 38 and 40.	1. ***Only the*** national members of Eurojust and their assistants shall, ***where necessary to fulfil*** their mandate, have the right to access and search data entered in SIS within their mandate, in accordance with Articles 26, 32, 34**,** 38 and 40.
597	2. Where a search by a national member of Eurojust reveals the existence of an alert in SIS, he or she shall inform the issuing Member State.	2. Where a search by a national member of Eurojust reveals the existence of an alert in SIS, ***the national member*** shall ***immediately*** inform the issuing Member State.	2. Where a search by a national member of Eurojust reveals the existence of an alert in SIS, he or she shall inform the issuing Member State **thereof**. **Any communication of information obtained from such**	2. Where a search by a national member of Eurojust reveals the existence of an alert in SIS, he or she shall inform the issuing Member State **thereof**. **[Any communication of information obtained from such**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			a search may only be communicated to third countries and third bodies with the consent of the issuing Member State.	**a search may only be communicated to third countries and third bodies with the consent of the issuing Member State.]** Presidency to come back.
598	3. Nothing in this Article shall be interpreted as affecting the provisions of Decision 2002/187/JHA concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, or as affecting the powers of the Joint Supervisory Body set up pursuant to that Decision.	3. ***This*** Article ***is without prejudice to*** the provisions of Decision 2002/187/JHA concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, ***and to*** the powers of the Joint Supervisory Body set up pursuant to that Decision.	3. Nothing in this Article shall be interpreted as affecting the provisions of Decision 2002/187/JHA concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, or as affecting the powers of the Joint Supervisory Body set up pursuant to that Decision.	3. ***This*** Article ***is without prejudice to*** the provisions of Decision 2002/187/JHA concerning data protection and the liability for any unauthorised or incorrect processing of such data by national members of Eurojust or their assistants, ***and to*** the powers of the Joint Supervisory Body set up pursuant to that Decision.
599	4. Every access and search made by a national member of Eurojust or an assistant shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be logged.	4. ***For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity, Eurojust shall keep logs of every*** access ***to*** and search ***in SIS*** made by a national member of Eurojust or an assistant ***in accordance with the provisions of Article 12. Such logs*** shall ***show, in particular, the date and time of the data processing activity, the type of data used to perform a***	4. Every access and search made by a national member of Eurojust or an assistant shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be logged.	LIBE proposal: (2018-04-13) 4. ***For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity, Eurojust*** sh**all** keep logs of every access to and search in SIS made by a national member of Eurojust or an assistant **in accordance with the provisions of Article 12**. ***Such logs and***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		search, a reference to the type of data processed and the name of the person responsible for processing the data. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.		***documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.***
600	5. No parts of SIS shall be connected to any computer system for data collection and processing operated by or at Eurojust nor shall the data contained in SIS to which the national members or their assistants have access be transferred to such a computer system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be an unlawful download or copying of SIS data.		5. No parts of SIS shall be connected to any computer system for data collection and processing operated by or at Eurojust nor shall the data contained in SIS to which the national members or their assistants have access be transferred to such a computer system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be an unlawful download or copying of SIS data.	5. No parts of SIS shall be connected to any computer system for data collection and processing operated by or at Eurojust nor shall the data contained in SIS to which the national members or their assistants have access be transferred to such a computer system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be an unlawful download or copying of SIS data.
601	6. Access to data entered in SIS shall be limited to the national members and their assistants and shall not be extended to Eurojust staff.	***deleted***	6. Access to data entered in SIS shall be limited to the national members and their assistants and shall not be extended to Eurojust staff.	***deleted***
602	7. Measures to ensure security and confidentiality as provided for	7. Measures to ensure security and confidentiality as provided for in Articles 10 and 11 shall be	7. Measures to ensure security and confidentiality as provided for	7. Measures to ensure security and confidentiality as provided for

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	in Articles 10 and 11 shall be adopted and applied.	adopted and applied.	in Articles 10 and 11 shall be adopted and applied.	in Articles 10 and 11 shall be adopted and applied.
603	*Article 48*	*Article 48*	*Article 48*	*Article 48*
604	*Access to SIS data by the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support team*	*Access to SIS data by the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support team*	*Access to SIS data by the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support teams*[143]	
605	1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams shall, within their mandate, have the right to access and search data entered in SIS within their mandate.	1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, ***the members of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624*** as well as the members of the migration management support teams shall, within their mandate, have the right to access and search data entered in SIS ***in accordance with this Regulation***. ***They shall have this right only insofar as it is necessary for the performance of their tasks and insofar as required by the operational plan for a specific operation.***	1. ~~In accordance with Article 40(8) of Regulation (EU) 2016/1624,~~ **The** members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams**, set up in accordance with Articles 18, 20 and 32 of Regulation (EU) 2016/1624** shall, within their mandate **and provided that they are authorised to carry out checks in accordance with Article 43**, have the right to access and search data entered in SIS ~~within their mandate~~**. Access to data entered in SIS shall not be**	Adjusted LIBE proposal (outcome of drafting meeting of 13 April): 1. In accordance with Article 40(8) of Regulation (EU) 2016/1624, the members of ***the*** ~~European Border and Coast Guard~~ ***teams*** ~~or teams of staff involved in return-related tasks~~ ***as defined in Article 2(8) of Regulation (EU) 2016/1624*** as well as the members of the migration management support teams**, referred to in** ~~**set up in accordance with Articles 18, 20 and 32**~~ **of Regulation (EU) 2016/1624,** shall, within their mandate **and provided that they are authorised to carry out checks in accordance with Article 43 and have received the required training**, have the right to access and search data

[143] In plural as in Regulation (EU) 2018/…

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			extended to any other team members. [144]	entered in **SIS in so far it is necessary for the performance of their task and as required by the operational plan for a specific operation**. **Access to data entered in SIS shall not be extended to any other team members.**
606	2. Members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams shall access and search data entered in SIS in accordance with paragraph 1 via the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to in Article 49(1).	2. ***Members of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624*** as well as the members of the migration management support teams shall access and search data entered in SIS in accordance with paragraph 1 via the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to in Article 49(1).	2. Members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams shall **exercise this right to** access and search data entered in SIS in accordance with paragraph 1 via the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to in Article 49(1).	Adjusted LIBE proposal (outcome of drafting meeting of 13 April): 2. Members of the teams ***referred to in paragraph 1 ~~as defined in Article 2(8) of Regulation (EU) 2016/1624~~*** ~~as well as the members of the migration management support teams~~ shall **exercise this right to** access and search data entered in SIS in accordance with paragraph 1 via the technical interface set up and maintained by the European Border and Coast Guard Agency as referred to in Article 32(2).
607	3. Where a search by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support team reveals the existence of an alert in SIS, the issuing Member	3. Where a search by a ***member of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624*** or by a member of the migration management support team reveals the existence of an alert in SIS, the issuing Member State shall be informed thereof	3. Where a search by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support team**s** reveals the existence of an alert in SIS, the issuing Member	Outcome of drafting meeting of 13 April: 3. Where a search by a member of ***the teams referred to in paragraph 1, ~~as defined in Article 2(8) of Regulation (EU) 2016/1624 or by a member of the migration management support teams~~*** reveals

[144] Text moved from paragraph 5.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	State shall be informed thereof. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.	***immediately***. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating ***and only where they have the power to do so under Article 40(1) of Regulation (EU) 2016/1624***. The host Member State may authorise members of the teams to act on its behalf.	State shall be informed thereof. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.	the existence of an alert in SIS, the issuing Member State shall be informed thereof ***~~immediately~~***. In accordance with Article 40 of Regulation (EU) 2016/1624, members of the teams may only act in response to an alert in SIS under instructions from and, as a general rule, in the presence of border guards or staff involved in return-related tasks of the host Member State in which they are operating. The host Member State may authorise members of the teams to act on its behalf.
608	4. Every instance of access and every search made by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support team shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be logged.	4. ***For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity the European Border and Coast Guard Agency shall keep logs of*** every ***access to and*** search ***in SIS*** made by a ***member of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624*** or by a member of the migration management support ***teams. Such logs shall show, in particular, the date and time of the data processing activity, the type of data used to perform a search, a reference to the type of***	4. Every instance of access and every search made by a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support team**s** shall be logged in accordance with the provisions of Article 12 and every use made by them of data accessed by them shall be logged.	Outcome of drafting meeting of 13 April (similar text to Art. 30(9) Borders proposal): 4. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data security and integrity the teams referred to in paragraph 1 shall keep logs of every access to and search in SIS in accordance with the provisions of Article 12. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		data processed and the name of the person responsible for processing the data. Such logs and documentation shall not be considered to be the unlawful downloading or copying of any part of SIS. The content, retention period and rules and formats for the logs are defined in accordance with Article 12.		
609	5. Access to data entered in SIS shall be limited to a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support team and shall not be extended to any other team members.	5. Access to data entered in SIS shall be limited to a member ***of the teams as defined in Article 2(8) of Regulation (EU) 2016/1624*** or by a member of the migration management support team ***provided that they have received the required training. The access*** shall not be extended to any other team members.	5. ~~Access to data entered in SIS shall be limited to a member of the European Border and Coast Guard teams or teams of staff involved in return-related tasks or by a member of the migration management support team and shall not be extended to any other team members.~~[145]	Outcome of drafting meeting of 13 April: (deleted)
610	6. Measures to ensure security and confidentiality as provided for in Articles 10 and 11 shall be adopted and applied.	6. Measures to ensure security and confidentiality as provided for in Articles 10**,** 11**,** ***13 and 14*** shall be adopted and applied.	6. **The European Border and Coast Guard teams or teams of staff involved in return-related tasks or members of the migration management support teams shall take m**easures to ensure security and confidentiality	Presidency compromise proposal (text similar to Art. 30(5) Borders proposal): 6. **The teams referred to in paragraph 1, ~~European Border and Coast Guard Agency~~ shall adopt and apply ~~take~~ M**measures to ensure security, ~~and~~ confidentiality and self-monitoring~~.~~ as provided for in Articles 10**,** ~~and~~ 11~~,~~ ***and. 13.***

[145] Merged with paragraph 1.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			as provided for in Articles 10 and 11 ~~shall be adopted and applied.~~	***Its staff authorised to process SIS data shall receive appropriate training and information in accordance with ~~and~~ Article 14(1).*** ~~shall ***apply mutatis mutandis.*** be adopted and applied~~.
611	*Article 49*	*Article 49*	*Article 49*	*Article 49*
612	*Access to SIS data by the European Border and Coast Guard Agency*	*Access to SIS data by the European Border and Coast Guard Agency*	*Access to SIS data by the European Border and Coast Guard Agency*	*Access to SIS data by the European Border and Coast Guard Agency*
613	1. For the purposes of Article 48(1) and paragraph 2 of this Article the European Border and Coast Guard Agency shall set up and maintain a technical interface which allows a direct connection to Central SIS.	1. For the purposes of Article 48(1) the European Border and Coast Guard Agency shall set up and maintain a technical interface which allows a direct connection to Central SIS.	1. For the purposes of Article 48(1) **[**and ~~paragraph 2 of this~~ Article **49A]** the European Border and Coast Guard Agency shall set up and maintain a technical interface which allows a direct connection to Central SIS.	LIBE would provide further explanations. To be further discussed in the context of Art. 71.
614	2. The European Border and Coast Guard Agency shall, for the purpose of performing its tasks conferred on it by the Regulation establishing a European Travel Information and Authorisation System (ETIAS), have the right to access and search data entered in SIS, in accordance with Articles 26, 32, 34, 36 and 38(2) (j) and (k).	***[***2. ***Duly authorised staff of the ETIAS Central Unit established within the*** European Border and Coast Guard Agency shall, ***insofar as it is necessary*** for the purpose of performing ***any*** tasks conferred on it by the Regulation establishing a European Travel Information and Authorisation System (ETIAS), have the right to access and ***verify***	2.[146] ~~The European Border and Coast Guard Agency shall, for the purpose of performing its tasks conferred on it by the Regulation establishing a European Travel Information and Authorisation System (ETIAS), have the right to access and search data entered in SIS, in accordance with Articles 26, 32, 34, 36 and 38(2) (j) and (k).~~	***deleted***

[146] Paragraph moved to Article 49A(1).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		data entered in SIS, in accordance with Articles 26, 32, 34, 36 and 38(2) (j) and (k).***]***		
615	3. Where a verification by the European Border and Coast Guard Agency reveals the existence of an alert in SIS the procedure set out in Article 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.	***deleted***	3.[147] ~~Where a verification by the European Border and Coast Guard Agency reveals the existence of an alert in SIS the procedure set out in Article 22 of Regulation establishing a European Travel Information and Authorisation System (ETIAS) applies.~~	***deleted***
616	4. Nothing in this Article shall be interpreted as affecting the provisions of Regulation (EU) 2016/1624 concerning data protection and the liability for any unauthorised or incorrect processing of such data by the European Border and Coast Guard Agency.	4. Nothing in this Article shall be interpreted as affecting the provisions of Regulation (EU) 2016/1624 concerning data protection and the liability for any unauthorised or incorrect processing of such data by the European Border and Coast Guard Agency.	4. Nothing in this Article shall be interpreted as affecting the provisions of Regulation (EU) 2016/1624 concerning data protection and the liability for any unauthorised or incorrect processing of such data by the European Border and Coast Guard Agency.	4. Nothing in this Article shall be interpreted as affecting the provisions of Regulation (EU) 2016/1624 concerning data protection and the liability for any unauthorised or incorrect processing of such data by the European Border and Coast Guard Agency.
617	5. Every instance of access and every search made by the European Border and Coast Guard Agency shall be logged in accordance with the provisions of Article 12 and each use made of	***deleted***	5. Every instance of access and every search made by the European Border and Coast Guard Agency shall be logged in accordance with the provisions of Article 12 and each use made of	Connected to paragraph 1. To be further discussed.

[147] Paragraph moved to Article 49A(2).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	data accessed by them shall be registered.		data accessed by them shall be ~~registered~~ **logged**.	
618	6. Except where necessary to perform the tasks for the purposes of the Regulation establishing a European Travel Information and Authorisation System (ETIAS), no parts of SIS shall be connected to any computer system for data collection and processing operated by or at the European Border and Coast Guard Agency, nor shall the data contained in SIS to which the European Border and Coast Guard Agency has access be transferred to such a system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS data.	***deleted***	6. **Except in cases where paragraph 1 of this Article applies**, no parts of SIS shall be connected to any computer system for data collection and processing operated by or at the European Border and Coast Guard Agency, nor shall the data contained in SIS to which the European Border and Coast Guard Agency has access be transferred to such a system. No part of SIS shall be downloaded. The logging of access and searches shall not be construed to be the downloading or copying of SIS data.	To be further discussed; possibly turn it to a positive wording allowing read only (search) access to EBCG.
619	7. Measures to ensure security and confidentiality as provided for in Articles 10 and 11 shall be adopted and applied by the European Border and Coast Guard Agency.	7. Measures to ensure security and confidentiality as provided for in Articles 10**,** 11***, 13 and 14*** shall be adopted and applied by the European Border and Coast Guard Agency.	7. **The European Border and Coast Guard Agency shall take m**easures to ensure security and confidentiality as provided for in Articles 10 and 11 ~~shall be adopted and applied by the European Border and Coast Guard Agency~~**.**	LIBE proposal: 9. **The European Border and Coast Guard Agency shall take** ~~M~~**m**easures to ensure security and confidentiality. ~~as provided for in~~ Articles 10**,** ~~and~~ 11 ***, 13 and 14(1)*** shall ***apply mutatis mutandis.*** ~~be adopted and applied~~.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				(to be checked in connection with Art. 31(9) of Borders proposal)
620			***[Article 49A***[148]	***Article 49A*** ***Article deleted.***
621			***Access to SIS data by the ETIAS Central Unit***	
622			**1. The European Border and Coast Guard Agency shall, for the purpose of performing its tasks conferred on it by the Regulation establishing a European Travel Information and Authorisation System (ETIAS), have the right to access and search data entered in SIS, in accordance with Articles 26, 32, 34, 36 and 38(2)(j) and (k).**	
623			**2. Where a verification by the European Border and Coast Guard Agency reveals the existence of an alert in SIS the procedure set out in Articles 18, 20A and 22 of Regulation establishing a European Travel**	

[148] Provisions moved from Article 49(2) and (3).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			Information and Authorisation System (ETIAS) applies.][149]	
624			***Article 49B***	To be further discussed.
625			***Evaluation of the use of SIS by Europol, Eurojust and the European Border and Coast Guard Agency***	
626			**1. The Commission shall carry out an evaluation of the operation and the use of SIS in accordance with this Regulation by Europol, Eurojust and the European Border and Coast Guard Agency at least every five years.**	
627			**2. A team responsible for this on-site evaluation shall consist of a maximum of two Commission representatives, assisted by a maximum of eight experts designated by Member States.**	
628			**3. The Commission shall draw up an evaluation report following each evaluation, in**	

[149] The content and or the insertion of these provisions depend on the final text of the proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624 (see 10017/17), and its date of entry into force.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			consultation with the designated Member State experts. The evaluation report shall be based on the findings of the on-site evaluation team and shall analyse the qualitative, quantitative, operational, administrative and organisational aspects of the operation and use of SIS, as appropriate, and shall list any deficiencies identified during the evaluation.	
629			**4. Europol, Eurojust and the European Border and Cost Guard Agency respectively, shall be given the opportunity to make comments prior to the adoption of the report.**	
630			**5. The evaluation report shall be sent to the European Parliament and to the Council. The evaluation report shall be classified as EU RESTRICTED/RESTREINT UE in accordance with applicable security rules. Classification shall not preclude information being made available to the European Parliament.**	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
631			**6. <u>In light of the findings and the assessments contained in that evaluation report, the Commission shall draft recommendations for remedial action aimed at addressing any deficiencies identified during the evaluation and give an indication of the priorities for implementing them, as well as, where appropriate, examples of good practices.</u>**	
632			**7. <u>Following an evaluation, Europol, Eurojust and the European Border and Coast Guard Agency shall provide the Commission with an action plan to remedy any deficiencies identified in the evaluation report and shall thereafter continue to report on progress every three months until the action plan is fully implemented.</u>**	
633	*Article 50*		*Article 50*	*Article 50*
634	*Scope of access*		*Scope of access*	*Scope of access* (To be further discussed)
635	End-users, including Europol, the national members of Eurojust and		End-users, including Europol, the national members of Eurojust and	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	their assistants as well as the European Border and Coast Guard Agency may only access data which they require for the performance of their tasks.		their assistants**,** ~~as well as~~ the European Border and Coast Guard Agency**–, the members of the European Border and Coast Guard teams or teams of staff involved in return-related tasks as well as the members of the migration management support teams** may only access data which they require for the performance of their tasks.	
636	*Article 51*	*Article 51*	*Article 51*	*Article 51*
637	*Retention period of alerts*	***Review** period of alerts*	Retention period of alerts **- persons**[150]	**Review** period of alerts - **persons** 2018-04-13
638	1. Alerts entered in SIS pursuant to this Regulation shall be kept only for the time required to achieve the purposes for which they were entered.	1. Alerts entered in SIS pursuant to this Regulation shall ***not*** be kept ***longer than*** for the time required to achieve the purposes for which they were entered.	1. Alerts **on persons** entered in SIS pursuant to this Regulation shall be kept only for the time required to achieve the purposes for which they were entered.	1. Alerts **on persons** entered in SIS pursuant to this Regulation [***shall be kept only/not be kept longer than]*** for the time required to achieve the purposes for which they were entered.
639	2. A Member State issuing an alert shall, within five years of its entry into SIS, review the need to retain it. Alerts issued for the purposes of Article 36 of this	2. A Member State issuing an alert shall, within ***three*** years of its entry into SIS, review the need to retain it. Alerts issued for the purposes of Article 36 of this Regulation shall be ***reviewed within*** a maximum period of one	2. **Concerning alerts on persons:** **a) A Member State may issue an alert for a period of five years.**	2. **Concerning alerts on persons:** **a) A Member State may issue an alert for a period of [five/three] years.**

150 A new Article 51A was incorporated to rule the retention period of alerts on objects.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Regulation shall be kept for a maximum period of one year.	year.	**(b)** ~~A~~ **The issuing** Member State ~~issuing an alert~~ shall, within five years of **the alert's** ~~its~~ entry into SIS, review the need to retain it. ~~Alerts issued for the purposes of Article 36 of this Regulation shall be kept for a maximum period of one year.~~[151]	**b) The issuing** Member State shall, within five years of **the alert's** entry into SIS, review the need to retain it.
640	3. Alerts on blank official documents and issued identity documents entered in accordance with Article 38 shall be kept for a maximum of 10 years. Shorter retention periods for categories of object alerts may be established by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).	3. Alerts on blank official documents and issued identity documents entered in accordance with Article 38 shall be kept for a maximum of 10 years. ***Alerts on other objects issued in accordance with Articles 36 and 38 shall be kept for a maximum period of five years. The Commission shall be empowered to adopt a delegated act*** in accordance with ***Article 71a concerning shorter retention periods for categories of object alerts***.	3. ~~Alerts on blank official documents, and issued identity documents entered in accordance with Article 38 shall be kept for a maximum of 10 years.Shorter retention periods for categories of object alerts may be established by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).~~	**(deleted)** 2018-04-13
641			**By way of derogation to paragraph 2, concerning** alerts issued for the purposes of **Article**	**By way of derogation to paragraph 2, concerning** alerts issued for the purposes of **Article**

[151] Moved to paragraph 3.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			32 (2)(c) and (d) and Article 36 of this Regulation[152]**:** **(a) A Member State may issue an alert for a period of one year.** **(b) The issuing Member State shall, within one year of the alert's entry into SIS, review the need to retain it.**	**32 (2)(c) and (d) and** Article 36 of this Regulation[153]**:** **(a) A Member State may issue an alert for a period of one year.** **(b) The issuing Member State shall, within one year of the alert's entry into SIS, review the need to retain it.** Cross-references to be checked (2018-04-13)
642	4. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.		4. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.	4. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law. 2018-04-13
643	5. In cases where it becomes clear to staff in the SIRENE Bureau, who are responsible for coordinating and verifying of data quality, that an alert on a person has achieved its purpose and should be deleted from SIS, the staff shall notify the authority which created the alert to bring this issue to the attention of the authority. The authority shall have	5. ***As soon as*** it becomes clear to staff in the SIRENE Bureau, who are responsible for coordinating and verifying of data quality, that an alert on a person ***or an object*** has achieved its purpose and should be deleted from SIS, the staff shall ***immediately*** notify the authority which created the alert to bring this issue to the attention of the authority. The	5. ~~In cases where it becomes clear to staff in the SIRENE Bureau, who are responsible for coordinating and verifying of data quality, that an alert on a person has achieved its purpose and should be deleted from SIS, the staff shall notify the authority which created the alert to bring this issue to the attention of the authority. The authority shall have 30 calendar~~	**5. Within the review period, the issuing Member State may, following a comprehensive individual assessment, which shall be recorded, decide to keep the alert longer, should this prove necessary [and proportionate] for the purposes for which the alert on a person was issued. In such a case paragraph 2(a) or paragraph 3(a) as appropriate,**

[152] Text partially moved from paragraph 2.
[153] Text partially moved from paragraph 2.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	30 calendar days from the receipt of this notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the 30-day period expires without such a reply the alert shall be deleted by the staff of the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.	authority shall have ***seven*** calendar days from the receipt of ***that*** notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the ***seven***-day period expires without such a reply the alert shall be deleted by the staff of the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.	~~days from the receipt of this notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the 30-day period expires without such a reply the alert shall be deleted by the staff of the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.~~[154] **Within the review period, the issuing Member State may, following a comprehensive individual assessment, which shall be recorded, decide to keep the alert longer, should this prove necessary for the purposes for which the alert on a person was issued. In such a case paragraph 2(a) or paragraph 3(a) as appropriate, shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.**[155]	**shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.**[156]
644	6. Within the review period, the Member State issuing the alert	6. Within the review period, the Member State issuing the alert may, following a comprehensive	6. ~~Within the review period, the Member State issuing the alert~~	

154 Moved to paragraph 8.
155 Moved from paragraph 2a.
156 Moved from paragraph 2a.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	may, following a comprehensive individual assessment, which shall be logged, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued. In such a case paragraph 2 shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.	individual assessment, which shall be logged, decide to keep the alert longer, should this prove necessary ***and proportionate*** for the purposes for which the alert was issued. In such a case paragraph 2 shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.	~~may, following a comprehensive individual assessment, which shall be logged, decide to keep the alert longer, should this prove necessary for the purposes for which the alert was issued. In such a case paragraph 2 shall apply also to the extension. Any extension of an alert shall be communicated to CS-SIS.~~[157] Alerts shall automatically be ~~erased~~**deleted** after the review period referred to in paragraphs 2**(b) and 3(b)** except where the **issuing** Member has informed CS-SIS about the extension of the alert **on a person** pursuant to paragraph **5**. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.[158]	2018-04-13 6. Alerts shall automatically be ~~erased~~**deleted** after the review period referred to in paragraphs 2**(b) and 3(b)** except where the **issuing** Member has informed CS-SIS about the extension of the alert **on a person** pursuant to paragraph **5**. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.[159]
645	7. Alerts shall automatically be erased after the review period referred to in paragraph 2 except where the Member State issuing the alert has informed CS-SIS		7. ~~Alerts shall automatically be erased after the review period referred to in paragraph 2 except where the Member State issuing the alert has informed CS-SIS about the~~	

[157] Moved to paragraph 2a.
[158] Moved from paragraph 7.
[159] Moved from paragraph 7.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	about the extension of the alert pursuant to paragraph 6. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.		~~extension of the alert pursuant to paragraph 6. CS-SIS shall automatically inform the Member States of the scheduled deletion of data from the system four months in advance.~~ [160] Member States shall keep statistics about the number of alerts **on persons** for which the retention period has been extended in accordance with paragraph ~~6~~**5**.[161]	LIBE proposal (2018-04-13) Member States shall keep statistics about the number of alerts **on persons** for which the retention period has been extended in accordance with paragraph ~~6~~**5** [**and transmit them to the supervisory authorities referred to in Article 67.**][162]
646	8. Member States shall keep statistics about the number of alerts for which the retention period has been extended in accordance with paragraph 6.	8. Member States shall keep statistics about the number of alerts for which the retention period has been extended in accordance with paragraph 6 ***and transmit them to the supervisory authorities referred to in Article 67***.	8. ~~Member States shall keep statistics about the number of alerts for which the retention period has been extended in accordance with paragraph 6.~~[163] In cases where it becomes clear to staff in the SIRENE Bureau, who are responsible for coordinating and verifying of data quality, that an alert on a person has achieved its purpose and should be deleted from SIS, the staff shall **bring this issue to the attention of** ~~notify~~ the authority which created the alert ~~to bring this issue to the attention of~~	LIBE proposal (2018-04-13) To be checked in connection with Art. 34 Borders proposal 8. In cases where it becomes clear to staff in the SIRENE Bureau, who are responsible for coordinating and verifying of data quality, that an alert on a person has achieved its purpose and should be deleted from SIS, the staff shall **bring this issue to the attention of** ~~notify~~ the authority which created the alert ~~to bring this issue to the attention of the authority~~. The authority shall have **fifteen** calendar days from the

160 Moved to paragraph 6.
161 Moved from paragraph 8.
162 Moved from paragraph 8.
163 Moved to paragraph 7.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
			~~the authority~~. The authority shall have 30 calendar days from the receipt of this notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the 30-day period expires without such a reply**,** the alert shall**, where permissible under national law,** be deleted by the staff of the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.[164]	receipt of this notification to indicate that the alert has been or shall be deleted or shall state reasons for the retention of the alert. If the **fifteen**-day period expires without such a reply**,** the alert shall**, where permissible under national law,** be deleted by the staff of the SIRENE Bureau. SIRENE Bureaux shall report any recurring issues in this area to their national supervisory authority.[165]
647			***Article 51A***[166]	***Article 51A***[167]
648			***Retention period of alerts - objects***	***Retention period of alerts - objects***
649			**1. Alerts on objects entered in SIS pursuant to this Regulation shall be kept only for the time required to achieve the purposes for which they were entered.**	(2018-04-13) **1. Alerts on objects entered in SIS pursuant to this Regulation shall be kept only for the time required to achieve the purposes for which they were entered.**

[164] Moved from paragraph 5.
[165] Moved from paragraph 5.
[166] This new Article regards specifically the retention period for alerts on objects, and mirrors, mutatis mutandis, the provisions on retention period of alerts on persons (Article 51).
[167] This new Article regards specifically the retention period for alerts on objects, and mirrors, mutatis mutandis, the provisions on retention period of alerts on persons (Article 51).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
650			**2. Concerning alerts on objects:**	**2. Concerning alerts on objects:**
651			**(a) a Member State may issue an alert for objects for a period of 10 years.**	**LIBE proposal:** **(a) a Member State may issue an alert for objects for a period of 10 years.** COM adjustments: (a) ~~a~~ **A** Member State may issue an alert for objects **in accordance with Article 38** for a period of 10 years.
652				COM proposal: **(aa) A Member State may issue an alert for objects in accordance with Article 36 for a period of 5 years.**
653			**(b) A Member State may issue an alert for other objects in accordance with Articles 26, 32, 34, 36 or 38 for a period of five years if they are linked to alerts on persons.**	LIBE proposal: (b) **A Member State may issue an alert for other objects in accordance with Articles 26, 32, 34 or 36 for a period of five years if they are linked to alerts on persons.** COM adjustments: (b) ~~A Member State may issue an~~ Alerts for ~~other~~ objects **issued** in

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				accordance with Articles 26 **(5)**, 32 **(7)**~~,~~ **and** 34 **(2) shall be reviewed pursuant to Art. 51 and they**~~,~~ ~~36 or 38~~ **shall only be kept for the time for which the alert on the person is issued** ~~for a period of five years if they are linked to alerts on persons~~**.**
654			**(c) The retention periods referred to in paragraphs 2(a) and (b) may be extended should this prove necessary for the purposes for which the alert was issued. In such cases paragraphs (2)(a) and (b) shall also apply to the extension.**	LIBE proposal: **(c) The retention periods referred to in paragraphs 2(a) and (b) may be extended should this prove necessary for the purposes for which the alert was issued. In such cases paragraphs (2)(a) and (b) shall also apply to the extension.** COM adjustments: (c) The retention periods referred to in paragraphs 2(a) and (~~b~~**aa**) may be extended should this prove necessary for the purposes for which the alert was issued. In such cases paragraphs (2)(a) and (~~b~~**aa**) shall also apply to the extension.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
655			**(d) Shorter retention periods for categories of object alerts may be established by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).**	2018-04-13 **(d) Shorter retention periods for categories of object alerts may be established by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).**
656			**3. Member States shall keep statistics about the number of alerts on objects for which the retention period has been extended in accordance with paragraph 2(c).**	2018-04-13 **3. Member States shall keep statistics about the number of alerts on objects for which the retention period has been extended in accordance with paragraph 2(c).**
657	**CHAPTER XIII**	**CHAPTER XIII**	**CHAPTER XIII**	**CHAPTER XIII**
658	**DELETION OF ALERTS**	**DELETION OF ALERTS**	**DELETION OF ALERTS**	**DELETION OF ALERTS**
659	*Article 52*	*Article 52*	*Article 52*	*Article 52*
660	*Deletion of alerts*	*Deletion of alerts*	*Deletion of alerts*	*Deletion of alerts*
661	1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted once the person has been surrendered or extradited to the competent authorities of the issuing	1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted once the person has been surrendered or extradited to the competent authorities of the issuing	1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted once the person has been surrendered or extradited to the competent authorities of the issuing	1. Alerts for arrest for surrender or extradition purposes pursuant to Article 26 shall be deleted once the person has been surrendered or extradited to the competent authorities of the issuing

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Member State. They may also be deleted where the judicial decision on which the alert was based has been revoked by the competent judicial authority according to national law.	Member State. They ***shall*** also be deleted where the judicial decision on which the alert was based has been revoked by the competent judicial authority according to national law.	Member State. They **shall**~~may~~ also be deleted where the judicial decision on which the alert was based has been revoked by the competent judicial authority according to national law.	Member State. They **shall**~~may~~ also be deleted where the judicial decision on which the alert was based has been revoked by the competent judicial authority according to national law.
662	2. Alerts for missing persons shall be deleted in accordance with the following rules:		2. Alerts for missing **persons, children at risk of abduction or vulnerable** persons **pursuant to Article 32** shall be deleted in accordance with the following rules:	
663	(a) Concerning missing children, pursuant to Article 32, an alert shall be deleted upon:		(a) Concerning missing children~~,~~ **and children at risk of abduction** ~~pursuant to Article 32~~, an alert shall be deleted upon:	
664	– the resolution of the case, such as when the child has been repatriated or the competent authorities in the executing Member State have taken a decision on the care of the child);		– the resolution of the case, such as when the child has been repatriated or the competent authorities in the executing Member State have taken a decision on the care of the child);	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
665	– the expiry of the alert in accordance with Article 51;		– the expiry of the alert in accordance with Article 51;	
666	– a decision by the competent authority of the issuing Member State; or		– a decision by the competent authority of the issuing Member State; or	
667	– the location of the child.	- the location ***and his or her placement under official protection***.	– ~~the location of the child.~~	
668	(b) Concerning missing adults pursuant to Article 32, where no protective measures are requested, an alert shall be deleted upon:		(b) Concerning missing adults ~~pursuant to Article 32~~, where no protective measures are requested, an alert shall be deleted upon:	
669	– the execution of the action to be taken (whereabouts ascertained by the executing Member State);		– the execution of the action to be taken (whereabouts ascertained by the executing Member State);	
670	– the expiry of the alert in accordance with Article 51; or		– the expiry of the alert in accordance with Article 51; or	
671	– a decision by the competent authority of		– a decision by the competent authority of	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	the issuing Member State.		the issuing Member State.	
672	(c) Concerning missing adults where protective measures are requested, pursuant to Article 32, an alert shall be deleted upon:		(c) Concerning missing adults where protective measures are requested~~, pursuant to Article 32,~~ an alert shall be deleted upon:	
673	– the carrying out of the action to be taken (person placed under protection);		– the carrying out of the action to be taken (person placed under protection);	
674	– the expiry of the alert in accordance with Article 51; or		– the expiry of the alert in accordance with Article 51; or	
675	– a decision by the competent authority of the issuing Member State.		– a decision by the competent authority of the issuing Member State.	
676			**(d) Concerning vulnerable persons who need to be prevented from travel for their own potection an alert shall be deleted upon:**	
677			– **the carrying out of the action to be taken (person placed under protection);**	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
678			– **the expiry of the alert in accordance with Article 51; or**	
679			– **a decision by the competent authority of the issuing Member State.**[168]	
680	Subject to national law, where a person has been interned following a decision by a competent authority an alert may be retained until that person has been repatriated.	***Without prejudice*** to ***the*** national law, where a person has been interned following a decision by a competent authority an alert may be retained until that person has been repatriated.	Subject to national law, where a person has been interned following a decision by a competent authority an alert may be retained until that person has been repatriated.	
681	3. Alerts on persons sought for a judicial procedure shall be deleted in accordance with the following rules:		3. ~~Alerts on persons sought for a judicial procedure shall be deleted in accordance with the following rules:~~	
682	Concerning alerts on persons sought for a judicial procedure pursuant to Article 34 an alert shall be deleted upon:		Concerning alerts on persons sought for a judicial procedure pursuant to Article 34 an alert shall be deleted upon:	
683	(a) the communication of the whereabouts of the person to the competent authority of the issuing Member State. Where the information		(a) the communication of the whereabouts of the person to the competent authority of the issuing Member State. Where the information	

[168] Text similar to that of point (c).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	forwarded cannot be acted upon the SIRENE Bureau of the issuing Member State shall inform the SIRENE Bureau of the executing Member State in order to resolve the problem;		forwarded cannot be acted upon the SIRENE Bureau of the issuing Member State shall inform the SIRENE Bureau of the executing Member State in order to resolve the problem;	
684	(b) the expiry of the alert in accordance with Article 51; or		(b) the expiry of the alert in accordance with Article 51; or	
685	(c) a decision by the competent authority of the issuing Member State.		(c) a decision by the competent authority of the issuing Member State.	
686	Where a hit has been achieved in a Member State and the address details were forwarded to the issuing Member State and a subsequent hit in that Member State reveals the same address details the hit shall be logged in the executing Member State but neither the address details nor supplementary shall be resent to the issuing Member State. In such cases the executing Member State shall inform the issuing Member State of the repeated hits and the issuing Member State shall	Where a hit has been achieved in a Member State and the address details were forwarded to the issuing Member State and a subsequent hit in that Member State reveals the same address details the hit shall be logged in the executing Member State but neither the address details nor supplementary shall be resent to the issuing Member State. In such cases the executing Member State shall inform the issuing Member State of the repeated hits and the issuing Member State shall ***carry out a comprehensive individual assessment of*** the need to maintain	Where a hit has been achieved in a Member State and the address details were forwarded to the issuing Member State and a subsequent hit in that Member State reveals the same address details the hit shall be ~~logged~~ **recorded** in the executing Member State but neither the address details nor supplementary **information** shall be resent to the issuing Member State. In such cases the executing Member State shall inform the issuing Member State of the repeated hits and the issuing	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	consider the need to maintain the alert.	the alert.	Member State shall consider the need to maintain the alert.	
687	4. Alerts on discreet, inquiry and specific checks shall be deleted in accordance with the following rules:		4. ~~Alerts on discreet, inquiry and specific checks shall be deleted in accordance with the following rules:~~	
688	Concerning alerts on discreet, inquiry and specific checks, pursuant to Article 36, an alert shall be deleted upon:		Concerning alerts on discreet, inquiry and specific checks, pursuant to Article 36, an alert shall be deleted upon:	
689	(a) the expiry of the alert in accordance with Article 51;		(a) the expiry of the alert in accordance with Article 51;	
690	(b) a decision to delete by the competent authority of the issuing Member State.		(b) a decision to delete by the competent authority of the issuing Member State.	
691		***(ba) completion of the check by an executing Member State.***		
692	5. Alerts on objects for seizure or use as evidence shall be deleted in accordance with the following rules:		5. ~~Alerts on objects for seizure or use as evidence shall be deleted in accordance with the following rules:~~	
693	Concerning deletion of alerts on objects for seizure or use as evidence in criminal proceedings pursuant to Article 38 an alert shall be deleted upon:		Concerning deletion of alerts on objects for seizure or use as evidence in criminal proceedings pursuant to Article 38 an alert shall be deleted upon:	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
694	(a) the seizure of the object or equivalent measure once the necessary follow-up exchange of supplementary information has taken place between SIRENE Bureaux or the object becomes subject of another judicial or administrative procedure;		(a) the seizure of the object or equivalent measure once the necessary follow-up exchange of supplementary information has taken place between SIRENE Bureaux or the object becomes subject of another judicial or administrative procedure;	
695	(b) the expiry of the alert; or		(b) the expiry of the alert; or	
696	(c) a decision to delete by the competent authority of the issuing Member State.		(c) a decision to delete by the competent authority of the issuing Member State.	
697	6. Alerts on unknown wanted persons pursuant to Article 40 shall be deleted in accordance with the following rules:	6. Alerts on unknown wanted persons pursuant to Article 40 shall be deleted ***upon***:	6. Alerts on unknown wanted persons pursuant to Article 40 shall be deleted in accordance with the following rules:	
698	7. (a) the identification of the person; or		~~7.~~ (a) the identification of the person; or	
699	8. (b) the expiry of the alert.	(b) the expiry of the alert ***in accordance with Article 51; or***	~~8.~~ (b) the expiry of the alert.	
700		***(ba) a decision to delete by the competent authority of the issuing Member State.***		
701		***6a. In addition to paragraphs 1 to 6 of this Article, alerts shall***		

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		also be deleted where necessary following the compatibility check provided for in Article 23a.		
702		***6b. Where an alert expires in accordance with Article 51, its deletion under paragraph 2 or 3 shall be carried out automatically.***		
703				COM proposal (2018-04-12): (7) Alerts for objects issued in accordance with Articles 26 (5), 32 (7), and 34 (2) shall be deleted when the alert on the person is deleted in accordance with paragraphs (1), (2) and (3) of this Article.
704	**CHAPTER XIV**	**CHAPTER XIV**	**CHAPTER XIV**	**CHAPTER XIV**
705	**GENERAL DATA PROCESSING RULES**	**GENERAL DATA PROCESSING RULES**	**GENERAL DATA PROCESSING RULES**	**GENERAL DATA PROCESSING RULES**
706	*Article 53*	*Article 53*	*Article 53*	*Article 53*
707	*Processing of SIS data*	*Processing of SIS data*	*Processing of SIS data*	*Processing of SIS data*
708	1. The Member States may process the data referred to in Article 20 only for the purposes laid down for each category of alert referred to in Articles 26, 32, 34, 36, 38 and 40.		1. The Member States may process the data referred to in Article 20 only for the purposes laid down for each category of alert referred to in Articles 26, 32, 34, 36, 38 and 40.	1. The Member States may process the data referred to in Article 20 only for the purposes laid down for each category of alert referred to in Articles 26, 32, 34, 36, 38 and 40.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
709	2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 43 to carry out a direct search. The provisions of this Regulation shall apply to such copies. A Member State shall not copy alert data or additional data entered by another Member State from its N.SIS or from the CS-SIS into other national data files.		2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 43 to carry out a direct search **or for the Agency to ensure uninterrupted availablity of the Central SIS**. The provisions of this Regulation shall apply to such copies. A Member State shall not copy alert data or additional data entered by another Member State from its N.SIS or from the CS-SIS into other national data files.	To be further discussed in the context of the discussion concerning Article 4.
710	3. Technical copies, as referred to in paragraph 2, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in the event of an emergency until the emergency comes to an end.	3. Technical copies, as referred to in paragraph 2, which lead to off-line databases may be retained for a period not exceeding 48 hours.	3. Technical copies, as referred to in paragraph 2, which lead to off-line databases may be retained for a period not exceeding 48 hours. That period may be extended in the event of an emergency until the emergency comes to an end.	To be further discussed. LIBE maintains its position.
711	4. Member States shall keep an up-to-date inventory of those copies, make that inventory available to their national supervisory authority, and ensure that the provisions of this Regulation, in particular those of	4. Member States shall keep an up-to-date inventory of those copies, make that inventory available to their national supervisory authority ***as well as the European Data Protection Supervisor***, and ensure that the	4. Member States shall keep an up-to-date inventory of those copies, make that inventory available to their national supervisory authority, and ensure that the provisions of this Regulation, in particular those of	4. Member States shall keep an up-to-date inventory of those copies, make that inventory available to their national supervisory authority, and ensure that the provisions of this Regulation, in particular those of

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Article 10, are applied in respect of those copies.	provisions of this Regulation, in particular those of Article 10, are applied in respect of those copies.	Article 10, are applied in respect of those copies.	Article 10, are applied in respect of those copies.
712	5. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 43 and to duly authorised staff.		5. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 43 and to duly authorised staff.	5. Access to data shall only be authorised within the limits of the competence of the national authorities referred to in Article 43 and to duly authorised staff.
713	6. With regard to the alerts laid down in Articles 26, 32, 34, 36, 38 and 40 of this Regulation, any processing of information contained therein for purposes other than those for which it was entered in SIS has to be linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the Member State issuing the alert shall be obtained for this purpose.		6. With regard to the alerts laid down in Articles 26, 32, 34, 36, 38 and 40 of this Regulation, any processing of information contained therein for purposes other than those for which it was entered in SIS has to be linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the Member State issuing the alert shall be obtained for this purpose.	6. With regard to the alerts laid down in Articles 26, 32, 34, 36, 38 and 40 of this Regulation, any processing of information contained therein for purposes other than those for which it was entered in SIS has to be linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious crime. Prior authorisation from the Member State issuing the alert shall be obtained for this purpose.
714	7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State.	7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State ***and subject to penalties in accordance with***	7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State.	7. Any use of data which does not comply with paragraphs 1 to 6 shall be considered as misuse under the national law of each Member State ***and subject to***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		Article 70a.		***penalties in accordance with Article 70a***. The use of word "misused" will be assessed throughout the text of the Regulation.
715	8. Each Member State shall send, to the Agency, a list of its competent authorities which are authorised to search directly the data contained in SIS pursuant to this Regulation, as well as any changes to the list. The list shall specify, for each authority, which data it may search and for what purposes. The Agency shall ensure the annual publication of the list in the *Official Journal of the European Union*.	8. Each Member State shall send to the Agency a list of its competent authorities which are authorised to search directly the data contained in SIS pursuant to this Regulation, as well as any changes to the list. The list shall specify, for each authority, which data it may search and for what purposes. The Agency shall ensure the annual publication of the list in the *Official Journal of the European Union*. ***The Commission shall maintain a public website containing this information. It shall ensure that the website is always up to date.***	8. Each Member State shall send, to the Agency, a list of its competent authorities which are authorised to search directly the data contained in SIS pursuant to this Regulation, as well as any changes to the list. The list shall specify, for each authority, which data it may search and for what purposes. The Agency shall ensure the annual publication of the list in the *Official Journal of the European Union*.	LIBE proposal: 8. Each Member State shall send to the Agency a list of its competent authorities which are authorised to search directly the data contained in SIS pursuant to this Regulation, as well as any changes to the list. The list shall specify, for each authority, which data it may search and for what purposes. The Agency shall ensure the annual publication of the list in the Official Journal of the European Union. ***eu-LISA shall maintain a continuously updated public website containing that information.***
716	9. In so far as Union law does not lay down specific provisions, the law of each Member State shall apply to data entered in its N.SIS.		9. In so far as Union law does not lay down specific provisions, the law of each Member State shall apply to data entered in its N.SIS.	9. In so far as Union law does not lay down specific provisions, the law of each Member State shall apply to data entered in its N.SIS.
717	*Article 54*		*Article 54*	*Article 54*
718	*SIS data and national files*		*SIS data and national files*	*SIS data and national files*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
719	1. Article 53(2) shall not prejudice the right of a Member State to keep in its national files SIS data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.		1. Article 53(2) shall not prejudice the right of a Member State to keep in its national files SIS data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.	1. Article 53(2) shall not prejudice the right of a Member State to keep in its national files SIS data in connection with which action has been taken on its territory. Such data shall be kept in national files for a maximum period of three years, except if specific provisions in national law provide for a longer retention period.
720	2. Article 53(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert issued in SIS by that Member State.		2. Article 53(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert issued in SIS by that Member State.	2. Article 53(2) shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert issued in SIS by that Member State.
721	*Article 55*	*Article 55*	*Article 55*	*Article 55*
722	*Information in case of non-execution of alert*	***Procedure** in case of non-execution of alert*	*Information in case of non-execution of alert*	
723	If a requested action cannot be performed, the requested Member State shall immediately inform the Member State issuing the alert.	If a requested action cannot be performed, ***the following procedure applies:***	If a requested action cannot be performed, the requested Member State shall immediately inform the **issuing** Member State ~~issuing the alert~~ **via the exchange of supplementary information**.	PRES compromise (SIRENE Manual, point 2.4): 1. If a requested action cannot be performed, the requested Member State shall immediately inform the **issuing** Member State ~~issuing the alert~~ **via the exchange of supplementary information**.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
724		***(a)*** the requested Member State shall immediately inform the issuing Member State ***via its SIRENE Bureau stating why not, in accordance with the SIRENE Manual;***		To be further discussed. Link to Sirene Manual. PRES compromise to delete.
725		***(b) the Member States concerned may agree on the action to be taken in line with the SIS legal instruments and their own national laws;***		To be further discussed. Link to Sirene Manual. PRES compromise to delete.
726		***(c) if a requested action cannot be carried out with regard to persons involved in an activity referred to in Directive (EU) 2017/541, the requested Member State shall immediately inform Europol.***		PRES compromise (SIRENE Manual, point 2.4): ***2. If a requested action cannot be carried out with regard to persons involved in an activity referred to in Directive (EU) 2017/541, the issuing Member State shall immediately inform Europol.***
727	*Article 56*	*Article 56*	*Article 56*	*Article 56*
728	*Quality of the data processed in SIS*	*Quality of the data processed in SIS*	*Quality of the data processed in SIS*	*Quality of the data processed in SIS*
729	1. A Member State issuing an alert shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS lawfully.		1. A**n issuing** Member State ~~issuing an alert~~ shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS lawfully.	1. A**n issuing** Member State ~~issuing an alert~~ shall be responsible for ensuring that the data are accurate, up-to-date and entered in SIS lawfully.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
730		***1a. Where an issuing Member State has relevant additional or modified data as listed in Article 20(3), the Member State shall complete or correct the alert immediately.***		PRES compromise (SIRENE Manual, point 2.12.3.): ***1a. Where an issuing Member State receives relevant additional or modified data as listed in Article 20(3), the Member State shall complete or correct the alert without delay.***
731		***1b. Where another Member State has relevant additional or modified alphanumeric data as listed in Article 20(3), that Member State shall transmit it immediately to the issuing Member to enable the latter to complete the alert.***		PRES compromise (SIRENE Manual, point 2.12.3.): ***1b. Where another Member State has relevant additional or modified ~~alphanumeric~~ data as listed in Article 20(3), that Member State shall transmit it ~~immediately without delay~~ to the issuing Member State to enable the latter to complete the alert. If the additional or modified data relate to persons they shall only be transmitted if the identity of the person is ascertained.***
732	2. Only the Member State issuing an alert shall be authorised to modify, add to, correct, update or delete data which it has entered.		2. Only the **issuing** Member State ~~issuing an alert~~ shall be authorised to modify, add to, correct, update or delete data which it has entered.	2. Only the **issuing** Member State ~~issuing an alert~~ shall be authorised to modify, add to, correct, update or delete data which it has entered.
733	3. Where a Member State other than that which issued an alert has evidence suggesting that an item of data is factually	3. Where a Member State other than that which issued an alert has evidence suggesting that an item of data is factually	3. Where a Member State other than that which issued an alert has evidence suggesting that an item of data is factually	To be further discussed. LIBE could consider a compromise of 4 days and 7 days.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	incorrect or has been unlawfully stored, it shall, through the exchange of supplementary information, inform the issuing Member State at the earliest opportunity and not later than 10 days after the said evidence has come to its attention. The issuing Member State shall check the communication and, if necessary, correct or delete the item in question without delay.	incorrect or has been unlawfully stored, it shall, through the exchange of supplementary information, inform the issuing Member State at the earliest opportunity and not later than ***two working*** days after the said evidence has come to its attention. The issuing Member State shall check the communication and, if necessary, correct or delete the item in question ***within seven working days from the notification***	incorrect or has been unlawfully stored, it shall, through the exchange of supplementary information, inform the issuing Member State at the earliest opportunity and not later than 10 days after the said evidence has come to its attention. The issuing Member State shall check the communication and, if necessary, correct or delete the item in question without delay.	
734	4. Where the Member States are unable to reach agreement within two months of the time when the evidence first came to light, as described in paragraph 3, the Member State which did not issue the alert shall submit the matter to the national supervisory authorities concerned for a decision.	4. Where the Member States are unable to reach agreement within two months of the time when the evidence first came to light, as described in paragraph 3, the Member State which did not issue the alert shall submit the matter to the national supervisory authorities ***and to the European Data Protection Supervisor*** concerned for a decision ***by means of cooperation under Article 69***.	4. Where the Member States are unable to reach agreement within two months of the time when the evidence first came to light, as described in paragraph 3, the Member State which did not issue the alert shall submit the matter to the **European Data Protection Supervisor who shall, jointly with the** national supervisory authorities concerned ~~for a decision~~**, act as a mediator**[169].	4. Where the Member States are unable to reach agreement within two months of the time when the evidence first came to light, as described in paragraph 3, the Member State which did not issue the alert shall submit the matter to the national supervisory authorities ***and to the European Data Protection Supervisor*** concerned for a decision ***by means of cooperation under Article 69***.

169 Text inspired on Article 49(4) of Council Decision 2007/533/JHA.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
735	5. The Member States shall exchange supplementary information where a person complains that he or she is not the person wanted by an alert. Where the outcome of the check shows that there are in fact two different persons the complainant shall be informed of the measures laid down in Article 59.	5. The Member States shall exchange supplementary information where a person complains that he or she is not the person wanted by an alert. Where the outcome of the check shows that there are in fact two different persons the complainant shall be informed of the measures laid down in Article 59 ***and of his or her right to redress in accordance with Article 66(1)***.	5. The Member States shall exchange supplementary information where a person complains that he or she is not the person wanted by an alert. Where the outcome of the check shows that there are in fact two different persons the complainant shall be informed of the measures laid down in Article 59.	5. The Member States shall exchange supplementary information where a person complains that he or she is not the person wanted by an alert. Where the outcome of the check shows that there are in fact two different persons the complainant shall be informed of the measures laid down in Article 59 ***and of his or her right to redress in accordance with Article 66(1)***.
736	6. Where a person is already the subject of an alert in SIS, a Member State which enters a further alert shall reach agreement on the entry of the alert with the Member State which entered the first alert. The agreement shall be reached on the basis of the exchange of supplementary information.	***deleted***	6. Where a person is already the subject of an alert in SIS, a Member State which enters a further alert shall **observe the compatability and priority of alerts and, where necessary, exchange supplementary information** ~~reach agreement on the entry of the alert with the Member State which entered the first alert. The agreement shall be reached on the basis of the exchange of supplementary information~~.	Moved to art. 23a
737	*Article 57*	*Article 57*	*Article 57*	*Article 57*
738	*Security incidents*	*Security incidents*	*Security incidents*	*Security incidents*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
739	1. Any event that has or may have an impact on the security of SIS and may cause damage or loss to SIS data shall be considered to be a security incident, especially where 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 SIS and may cause damage or loss to SIS data shall be considered to be a security incident, especially 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 SIS ~~and~~**or** may cause damage or loss to SIS data **or to the supplementary information** shall be considered to be a security incident, especially where 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 SIS ~~and~~**or** may cause damage or loss to SIS data **or to the supplementary information** shall be considered to be a security incident, especially where ***unlawful*** access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.
740	2. Security incidents shall be managed to ensure a quick, effective and proper response.		2. Security incidents shall be managed to ensure a quick, effective and proper response.	2. Security incidents shall be managed to ensure a quick, effective and proper response.
741	3. Member States shall notify the Commission, the Agency and the national supervisory authority of security incidents. The Agency shall notify the Commission and the European data Protection Supervisor of security incidents.	3. ***Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) No 2016/679 or to Article 30 of Directive (EU) No 2016/680,*** Member States shall notify the Commission, the Agency**,** the national supervisory authority ***and the European Data Protection Supervisor immediately*** of security incidents. ***In the event of a security incident on the Central SIS, the*** Agency shall notify the Commission and the European Data Protection	3. Member States**, Europol, Eurojust and the European Border and Coast Guard Agency** shall notify the Commission, the Agency and the national supervisory authority of security incidents. The Agency shall notify the Commission and the European ~~d~~**D**ata Protection Supervisor of security incidents.	Revised PRES compromise proposal: 3. ***Without prejudice to the notification and communication of a personal data breach pursuant to Article 33 of Regulation (EU) No 2016/679 or to Article 30 of Directive (EU) No 2016/680,*** Member States, **Europol, Eurojust and the European Border and Coast Guard Agency** shall notify the Commission, the Agency**,** ***the national supervisory authority*** and the European Data Protection Supervisor ***without delay*** of security incidents. ***In the event of a security incident on the Central SIS,*** the Agency, ~~**Europol and the European Border and Coast Guard**~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		Supervisor ***immediately*** of ***those*** security incidents.		**~~Agency~~** shall notify the Commission and the European Data Protection Supervisor ***without delay*** ~~of ***those*** security incidents~~.
742	4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent by other Member States shall be given to the Member States and reported in compliance with the incident management plan provided by the Agency.	4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent by other Member States, shall be provided to the Member States ***immediately*** and reported in compliance with the incident management plan provided by the Agency.	4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent by other Member States **or supplementary information exchanged** shall be given to **all** the Member States and reported in compliance with the incident management plan provided by the Agency.	4. Information regarding a security incident that has or may have an impact on the operation of SIS in a Member State or within the Agency or on the availability, integrity and confidentiality of the data entered or sent **or supplementary information exchanged** by other Member States, shall be provided to **all** the Member States ***without delay*** and reported in compliance with the incident management plan provided by the Agency.
743		***4a. The Member States and eu-LISA shall collaborate in the event of a security incident.***		***4a. The Member States and the Agency shall collaborate in the event of a security incident.***
744		***4b. In case of a data breach data subjects shall be informed in accordance with Article 34 of Regulation (EU) No 2016/679 or Article 31 of Directive (EU) No 2016/680.***		EP would consider to drop it, provided that 4a, 4c and 4d would remain.
745		***4c. The Commission shall report serious incidents immediately to the European Parliament and the Council.***		COM services addition of 12 March: 4c. The Commission shall report serious incidents immediately to the

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				European Parliament and the Council. ***These reports shall be classified as EU RESTRICTED/RESTREINT UE in accordance with applicable security rules.***
746		***4d. Where a security incident is caused by the misuse of data, Member States, Europol, Eurojust and the European Border and Coast Guard Agency shall ensure that penalties or disciplinary measures may be imposed in accordance with Article 70a.***		Provisionally agreed, but subject to the agreement regarding Art. 70a ***4d. Where a security incident is caused by the misuse of data, Member States, Europol, Eurojust and the European Border and Coast Guard Agency shall ensure that penalties or disciplinary measures may be imposed in accordance with Article 70a.***
747	*Article 58*	*Article 58*	*Article 58*	*Article 58*
748	*Distinguishing between persons with similar characteristics*	*Distinguishing between persons with similar characteristics*	*Distinguishing between persons with similar characteristics*	*Distinguishing between persons with similar characteristics*
749	Where it becomes apparent, when a new alert is entered, that there is already a person in SIS with the same identity description element, the following procedure shall apply:		Where it becomes apparent, when a new alert is entered, that there is already a person in SIS with the same identity description element, the following procedure shall apply:	Where it becomes apparent, when a new alert is entered, that there is already a person in SIS with the same identity description element, the following procedure shall apply:
750	(a) the SIRENE Bureau shall contact the requesting authority to clarify whether	(a) the SIRENE Bureau shall ***immediately*** contact the requesting authority to clarify whether or not the alert is on the same person;	(a) the SIRENE Bureau shall contact the requesting authority to clarify whether or	COM services proposal of 12 March: (a) the ~~**competent authority**~~ **SIRENE Bureau** shall contact ***[immediately]*** the ~~**requesting**~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	or not the alert is on the same person;		not the alert is on the same person; **and**	~~**authority**~~ issuing Member State **via the exchange of supplementary information** to clarify whether or not the alert is on the same person; **and**
751	(b) where the cross-check reveals that the subject of the new alert and the person already in SIS are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article 56(6). Where the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentifications.	(b) where the cross-check reveals that the subject of the new alert and the person already in SIS are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article ***23a***. Where the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentifications.	(b) where the cross-check reveals that the subject of the new alert and the person already in SIS are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article 56(6). Where the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentifications.	(b) where the cross-check reveals that the subject of the new alert and the person already in SIS are indeed one and the same, the SIRENE Bureau shall apply the procedure for entering multiple alerts as referred to in Article ***23a***. Where the outcome of the check is that there are in fact two different persons, the SIRENE Bureau shall approve the request for entering the second alert by adding the necessary elements to avoid any misidentifications.
752	*Article 59*	*Article 59*	*Article 59*	*Article 59*
753	*Additional data for the purpose of dealing with misused identities*	*Additional data for the purpose of dealing with misused identities*	*Additional data for the purpose of dealing with misused identities*	*Additional data for the purpose of dealing with misused identities*
754	1. Where confusion may arise between the person actually intended as the subject of an alert and a person whose identity has	1. Where confusion may arise between the person actually intended as the subject of an alert and a person whose identity has	1. Where confusion may arise between the person actually intended as the subject of an alert and a person whose identity has	1. Where confusion may arise between the person actually intended as the subject of an alert and a person whose identity has

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	been misused, the issuing Member State shall, subject to that person's explicit consent, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification.	been misused, the issuing Member State shall, subject to that person's explicit consent, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification. ***Any person whose identity has been misused has the right to withdraw his or her consent to the information being processed.***	been misused, the issuing Member State shall, subject to that person's explicit consent, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification.	been misused, the issuing Member State shall, subject to that person's explicit consent, add data relating to the latter to the alert in order to avoid the negative consequences of misidentification. ***Any person whose identity has been misused has the right to withdraw his or her consent to the information being processed.***
755	2. Data relating to a person whose identity has been misused shall be used only for the following purposes:		2. Data relating to a person whose identity has been misused shall be used only for the following purposes:	2. Data relating to a person whose identity has been misused shall be used only for the following purposes:
756	(a) to allow the competent authority to distinguish the person whose identity has been misused from the person actually intended as the subject of the alert;		(a) to allow the competent authority to distinguish the person whose identity has been misused from the person actually intended as the subject of the alert;	(a) to allow the competent authority to distinguish the person whose identity has been misused from the person actually intended as the subject of the alert;
757	(b) to allow the person whose identity has been misused to prove his or her identity and to establish that his or her identity has been misused.		(b) to allow the person whose identity has been misused to prove his or her identity and to establish that his or her identity has been misused.	(b) to allow the person whose identity has been misused to prove his or her identity and to establish that his or her identity has been misused.
758	3. For the purpose of this Article, only the following	3. For the purpose of this Article, ***and subject to the explicit consent of the person whose identity was misused for each data***	3. For the purpose of this Article, only the following personal data **of the person whose identity**	3. For the purpose of this Article, ***and subject to the explicit consent of the person whose identity was misused for each data category,*** only the

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	personal data may be entered and further processed in SIS:	***category,*** only the following personal data may be entered and further processed in SIS :	**has been misused** may be entered and further processed in SIS:	following personal data **of the person whose identity has been misused** may be entered and further processed in SIS:
759	(a) surname(s)		(a) surname~~(s)~~**;**	(a) surname~~(s)~~**;**
760	(b) forename(s),		(b) forename~~(s),~~**;**	(b) forename~~(s),~~**;**
761	(c) name(s) at birth		(c) name~~(s)~~ at birth**;**	(c) name~~(s)~~ at birth**;**
762	(d) previously used names and any aliases possibly entered separately;		(d) previously used names and any aliases possibly entered separately;	(d) previously used names and any aliases possibly entered separately;
763	(e) any specific objective and physical characteristic not subject to change;		(e) any specific objective**,** ~~and~~ physical characteristic not subject to change;	(e) any specific objective and physical characteristic not subject to change;
764	(f) place of birth		(f) place of birth;	(f) place of birth;
765	(g) date of birth;		(g) date of birth;	(g) date of birth;
766	(h) sex;	(h) ***gender***;	(h) ~~sex~~**gender**;	(h) ~~sex~~**gender**;
767	(i) photographs and facial images;		(i) photographs and facial images;	(i) photographs and facial images;
768	(j) fingerprints;		(j) ~~fingerprints~~**dactyloscopic data**;	To be further discussed.
769	(k) nationality(ies);		(k) nationality**/nationalit**~~(ies)~~;	(k) nationality**/nationalit**~~(ies)~~;

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
770	(l) the category of the person's identity document		(l) the category of the person's identi**fication**~~ty~~ document**s;**	(l) the category of the person's identi**fication**~~ty~~ document**s;**
771	(m) the country of issue of the person's identity document		(m) the country of issue of the person's ~~identity~~ **identification** document**s;**	(m) the country of issue of the person's ~~identity~~ **identification** document**s;**
772	(n) the number(s) of the person's identity document		(n) the number(s) of the person's ~~identity~~**identification** document**s;**	(n) the number(s) of the person's ~~identity~~**identification** document**s;**
773	(o) the date of issue of a person's identity document		(o) the date of issue of a person's i~~dentity~~**identification** document**s;**	(o) the date of issue of a person's i~~dentity~~**identification** document**s;**
774	(p) address of the victim;		(p) address of the **person**~~victim~~;	(p) address of the **person**~~victim~~;
775	(q) victim's father's name;		(q) **person**~~victim~~'s father's name;	(q) **person**~~victim~~'s father's name;
776	(r) victim's mother's name		(r) **person**~~victim~~'s mother's name**.**	(r) **person**~~victim~~'s mother's name**.**
777	4. The technical rules necessary for entering and further processing the data referred to in paragraph 3 shall be established by means of implementing measures laid down and developed in accordance with the examination procedure referred to in Article 72(2).		4. The technical rules necessary for entering and further processing the data referred to in paragraph 3 shall be established by means of implementing measures laid down and developed in accordance with the examination procedure referred to in Article 72(2).	4. The technical rules necessary for entering and further processing the data referred to in paragraph 3 shall be established by means of implementing measures laid down and developed in accordance with the examination procedure referred to in Article 72(2).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
778	5. The data referred to in paragraph 3 shall be deleted at the same time as the corresponding alert or earlier where the person so requests.	5. The data referred to in paragraph 3 shall be deleted ***as soon as this is requested by the person whose identity was misused or*** at the same time as the corresponding alert ***is deleted***.	5. The data referred to in paragraph 3 shall be deleted at the same time as the corresponding alert or earlier where the person so requests.	5. The data referred to in paragraph 3 shall be deleted at the same time as the corresponding alert or earlier where the person so requests.
779	6. Only the authorities having a right of access to the corresponding alert may access the data referred to in paragraph 3. They may do so for the sole purpose of avoiding misidentification.		6. Only the authorities having a right of access to the corresponding alert may access the data referred to in paragraph 3. They may do so for the sole purpose of avoiding misidentification.	6. Only the authorities having a right of access to the corresponding alert may access the data referred to in paragraph 3. They may do so for the sole purpose of avoiding misidentification.
780	*Article 60*		*Article 60*	*Article 60*
781	*Links between alerts*		*Links between alerts*	*Links between alerts*
782	1. A Member State may create a link between alerts it enters in SIS. The effect of such a link shall be to establish a relationship between two or more alerts.		1. A Member State may create a link between alerts it enters in SIS. The effect of such a link shall be to establish a relationship between two or more alerts.	1. A Member State may create a link between alerts it enters in SIS. The effect of such a link shall be to establish a relationship between two or more alerts.
783	2. The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the retention period of each of the linked alerts.		2. The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the retention period of each of the linked alerts.	2. The creation of a link shall not affect the specific action to be taken on the basis of each linked alert or the retention period of each of the linked alerts.
784	3. The creation of a link shall not affect the rights of access		3. The creation of a link shall not affect the rights of access	3. The creation of a link shall not affect the rights of access

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	provided for in this Regulation. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.		provided for in this Regulation. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.	provided for in this Regulation. Authorities with no right of access to certain categories of alerts shall not be able to see the link to an alert to which they do not have access.
785	4. A Member State shall create a link between alerts when there is an operational need.		4. A Member State shall create a link between alerts when there is an operational need.	4. A Member State shall create a link between alerts when there is an operational need.
786	5. Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or international obligations, it may take the necessary measures to ensure that there can be no access to the link from its national territory or by its authorities located outside its territory.		5. Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or international obligations, it may take the necessary measures to ensure that there can be no access to the link from its national territory or by its authorities located outside its territory.	5. Where a Member State considers that the creation by another Member State of a link between alerts is incompatible with its national law or international obligations, it may take the necessary measures to ensure that there can be no access to the link from its national territory or by its authorities located outside its territory.
787	6. The technical rules for linking alerts shall be laid down and developed in accordance with the examination procedure referred to in Article 72(2).		6. The technical rules for linking alerts shall be laid down and developed in accordance with the examination procedure referred to in Article 72(2).	6. The technical rules for linking alerts shall be laid down and developed in accordance with the examination procedure referred to in Article 72(2).
788	*Article 61*		*Article 61*	*Article 61*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
789	*Purpose and retention period of supplementary information*		*Purpose and retention period of supplementary information*	*Purpose and retention period of supplementary information*
790	1. Member States shall keep a reference to the decisions giving rise to an alert at the SIRENE Bureau in order to support the exchange of supplementary information.		1. Member States shall keep a reference to the decisions giving rise to an alert at the SIRENE Bureau in order to support the exchange of supplementary information.	1. Member States shall keep a reference to the decisions giving rise to an alert at the SIRENE Bureau in order to support the exchange of supplementary information.
791	2. Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS.		2. Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS.	2. Personal data held in files by the SIRENE Bureau as a result of information exchanged shall be kept only for such time as may be required to achieve the purposes for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS.
792	3. Paragraph 2 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.		3. Paragraph 2 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.	3. Paragraph 2 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert which that Member State has issued or to an alert in connection with which action has been taken on its territory. The period for which such data may be held in such files shall be governed by national law.
793	*Article 62*		*Article 62*	*Article 62*

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
794	*Transfer of personal data to third parties*		*Transfer of personal data to third parties*	*Transfer of personal data to third parties*
795	Data processed in SIS and the related supplementary information pursuant to this Regulation shall not be transferred or made available to third countries or to international organisations.		Data processed in SIS and the related supplementary information pursuant to this Regulation shall not be transferred or made available to third countries or to international organisations.	Data processed in SIS and the related supplementary information pursuant to this Regulation shall not be transferred or made available to third countries or to international organisations.
796	*Article 63*	*Article 63*	*Article 63*	
797	*Exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol*	*Exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol*	~~*Exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol*~~	
798	1. By way of derogation from Article 62, the passport number, country of issuance and the document type of stolen, misappropriated, lost or invalidated passports entered in SIS may be exchanged with members of Interpol by establishing a connection between SIS and the Interpol database on stolen or missing travel documents, subject to the conclusion of an Agreement between Interpol and the European Union. The Agreement shall provide that the transmission of data entered by a Member State	***deleted***	~~1. By way of derogation from Article 62, the passport number, country of issuance and the document type of stolen, misappropriated, lost or invalidated passports entered in SIS may be exchanged with members of Interpol by establishing a connection between SIS and the Interpol database on stolen or missing travel documents, subject to the conclusion of an Agreement between Interpol and the European Union. The Agreement shall provide that the transmission of data entered by a Member State~~	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	shall be subject to the consent of that Member State.		~~shall be subject to the consent of that Member State.~~	
799	2. The Agreement referred to in paragraph 1 shall foresee that the data shared shall only be accessible to members of Interpol from countries that ensure an adequate level of protection of personal data. Before concluding this Agreement, the Council shall seek the opinion of the Commission on the adequacy of the level of protection of personal data and respect of fundamental rights and liberties regarding the automatic processing of personal data by Interpol and by countries which have delegated members to Interpol.	***deleted***	~~2. The Agreement referred to in paragraph 1 shall foresee that the data shared shall only be accessible to members of Interpol from countries that ensure an adequate level of protection of personal data. Before concluding this Agreement, the Council shall seek the opinion of the Commission on the adequacy of the level of protection of personal data and respect of fundamental rights and liberties regarding the automatic processing of personal data by Interpol and by countries which have delegated members to Interpol.~~	
800	3. The Agreement referred to in paragraph 1 may also provide for access through SIS for the Member States to data from the Interpol database on stolen or missing travel documents, in accordance with the relevant provisions of this Decision governing alerts on stolen, misappropriated, lost and invalidated passports entered in SIS.	***deleted***	~~3. The Agreement referred to in paragraph 1 may also provide for access through SIS for the Member States to data from the Interpol database on stolen or missing travel documents, in accordance with the relevant provisions of this Decision governing alerts on stolen, misappropriated, lost and invalidated passports entered in SIS.~~	***deleted***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
801	**CHAPTER XV**	**CHAPTER XV**	**CHAPTER XV**	**CHAPTER XV**
802	**DATA PROTECTION**	**DATA PROTECTION**	**DATA PROTECTION**	**DATA PROTECTION**
803	*Article 64*	*Article 64*	*Article 64*	*Article 64*
804	*Applicable legislation*	*Applicable legislation*	*Applicable legislation*	*Applicable legislation* To be further discussed. EP would reserve its position in view of the current proposal to review Regº 45/2001. EP would provide wording, probably to be put in [square brackets]. COM could accept the removal of this Article.
805	1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the Agency under this Regulation.	1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the Agency, ***the European Border and Coast Guard and Eurojust*** under this Regulation	1. Regulation (EC) No 45/2001 shall apply to the processing of personal data by the Agency **and by the European Border and Coast Guard Agency** under this Regulation. **Regulation (EU) 2016/794 (Europol Regulation) shall apply to the processing of personal data by Europol under this Regulation. Decision 2002/187 (Eurojust) shall apply to the processing of personal data by Eurojust under this Regulation.**	Presidency would accept the deletion of last sentence.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
806	2. Regulation (EU) 2016/679 shall apply to the processing of personal data provided that national provisions transposing Directive (EU) 2016/680 do not apply.	2. Regulation (EU) 2016/679 shall apply to the processing of personal data ***under this Regulation unless such processing is carried out by the competent authorities of the Member States for the purposes of the prevention, detection, investigation or prosecution of criminal offences, the execution of criminal penalties or safeguarding against threats to public security.***	2. Regulation (EU) 2016/679 shall apply to the processing of personal data provided that ~~national provisions transposing~~ Directive (EU) 2016/680 do**es** not apply.	LIBE proposal: 2. Regulation **(EU)** 2016/679 shall apply to the processing of personal data by the authorities referred to in Article 29 of this Regulation ***with the exception of processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*** *[exact wording of Art. 1 of Directive 2016/680; formulation "with the exception of" from EES Regulation Art. 49(2)]* ~~provided that national provisions transposing Directive (EU) 2016/680 do**es** not apply.~~
807		***2a. National provisions transposing Directive (EU) 2016/680 shall apply to the processing of personal data under this Regulation by competent national authorities for the purposes of the prevention, detection, investigation or prosecution of criminal offences, the execution of criminal***		See under paragraph 3

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		penalties or safeguarding against threats to public security.		
808		***2b. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol pursuant to Article 46 of this Regulation.***		
809	3. For processing of data by competent national authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences of the execution of criminal penalties including the safeguarding against the prevention of threat to public security national provisions transposing Directive (EU) 2016/680 shall apply.	***deleted***	3. **National provisions transposing Directive (EU) 2016/680 shall apply** ~~F~~**f**or processing of data by competent national authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences o**r**~~f~~ the execution of criminal penalties including the safeguarding against the prevention of threat to public security ~~national provisions transposing Directive (EU) 2016/680 shall apply~~.	LIBE proposal: 3. ~~**National provisions transposing** **Directive (EU) 2016/680 shall apply~~ ~~for~~ ***to the*** processing of ***personal*** data by competent national authorities for the purposes of the prevention, investigation, detection~~,~~ or prosecution of criminal offences ***or*** ~~of~~ the execution of criminal penalties**,** including the safeguarding against ***and*** the prevention of ~~threat~~ ***threats*** to public security ~~national provisions transposing Directive (EU) 2016/680 shall apply~~. *[text aligned to police directive; the reference to "national provisions" is not necessary and also not mentioned in EES and ETIAS]*
810	*Article 65*	*Article 65*	*Article 65*	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
811	*Right of access, rectification of inaccurate data and erasure of unlawfully stored data*	*Right of access, rectification **and restriction** of inaccurate data and erasure of unlawfully stored data*	*Right of access, rectification of inaccurate data and erasure of unlawfully stored data*	*As the right of restriction is a right provided for in the Police Directive LIBE would like to maintain it*
812	1. The right of data subjects to have access to data relating to them entered in SIS and to have such data rectified or erasure shall be exercised in accordance with the law of the Member State before which they invoke that right.	1. ***Without prejudice to Articles 15, 16, 17 and 18 of Regulation (EU) 2016/679 any data subject shall have the right to access and obtain the*** data relating to ***him or her recorded in the*** SIS and ***may request that data relating to him or her which are inaccurate be*** rectified or ***completed and that data recorded unlawfully be erased and that data processing be restricted.***	1. The right of data subjects to have access to data relating to them entered in SIS and to have such data rectified or ~~erasure~~**erased** shall be exercised in accordance with the law of the Member State before which they invoke that right.	COM services proposal (27 February): ***Data subjects shall be able to exercise their rights in accordance with Articles 12, 15, 16 and 17 of Regulation (EU) 2016/679 and Articles 14, 15, 17 and 18 of Directive (EU) 2016/680.***
813		***1a. Where appropriate, Articles 14 to 18 of Directive (EU) 2016/680 shall apply.***		
814	2. If national law so provides, the national supervisory authority shall decide whether information is to be communicated and by what means.		2. ~~If national law so provides, the national supervisory authority shall decide whether information is to be communicated and by what means.~~	PRES proposal to delete. LIBE showed openness.
815	3. A Member State other than that which has issued an alert may communicate information concerning such data only if it first gives the Member State issuing the alert an opportunity to state its		3. A Member State other than that which has issued an alert may communicate information **to a data subject** concerning such data only ~~if it first gives the~~ **once each issuing** Member State ~~issuing~~**gives**	**COM services proposal of 23 Jan 2018:** **3. A Member State other than that which has issued an alert may communicate information to**

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	position. This shall be done through the exchange of supplementary information.		~~alert an~~ ~~opportunity to state~~ its **consent**~~position~~**.** This shall be done through the exchange of supplementary information.	**a data subject concerning such data only if it first gives the Member State issuing the alert an opportunity to state its position. This shall be done through the exchange of supplementary information. In case the issuing Member State does not respond within 30 days the Member State shall refer the data subject to the issuing Member State.** LIBE does not agree with this COM proposal
816	4. A Member State shall take a decision not to communicate information to the data subject, in whole or in part, in accordance with national law, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:		4. A Member State shall take a decision not to communicate information to the data subject, in whole or in part, in accordance with national law, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the ~~natural person~~**data subject** concerned, in order to:	4. A Member State shall take a decision not to communicate information to the data subject, in whole or in part, in accordance with national law, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the ~~natural person~~**data subject** concerned, in order to:

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
817	(a) avoid obstructing official or legal inquiries, investigations or procedures;		(a) avoid obstructing official or legal inquiries, investigations or procedures;	(a) avoid obstructing official or legal inquiries, investigations or procedures;
818	(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;		(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;	(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
819	(c) protect public security;		(c) protect public security;	(c) protect public security;
820	(d) protect national security;		(d) protect national security; **or**	(d) protect national security; **or**
821	(e) protect the rights and freedoms of others.		(e) protect the rights and freedoms of others.	(e) protect the rights and freedoms of others.
822		***In such cases, Member States shall provide for the controller to inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine a purpose under this paragraph. Member States***		COM services proposal (27 February): ***In such cases, the controller shall inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine a purpose under this paragraph. The controller shall inform the data subject of the possibility of lodging a complaint***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or of seeking a judicial remedy.		***with a supervisory authority or of seeking a judicial remedy.***
823		***Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.***		COM services proposal (27 February): ***The controller shall document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.***
824		***For such cases, Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authorities.***		***For such cases, Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authorities.***
825	5. Any person has the right to have factually inaccurate data relating to him rectified or unlawfully stored data relating to him erased.	***deleted***	5. ~~Any person has the right to have factually inaccurate data relating to him rectified or unlawfully stored data relating to him erased.~~	(deleted)
826	6. The person concerned shall be informed as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides.	6. The person concerned shall be informed as soon as possible and in any event not later than ***30*** days from the date on which he ***or she*** applies for access or sooner if national law so provides, ***regardless of whether the person***	6. ~~The person concerned~~ **Following an application for access, rectification or erasure, the data subject** shall be informed as soon as possible ~~and in any event not later than 60 days~~ from the date ~~on which he applies for access or~~	6. The person concerned shall be informed as soon as possible and in any event not later than ***30*** days from the date on which he ***or she*** applies for access or sooner if national law so provides***, regardless of whether the***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		is on Union territory or not.	~~sooner if national law so provides~~**of application, as to the follow-up given to the exercise of these rights**[170].	***person is ~~on Union territory~~*** **in a third-country** ***or not***.
827	7. The person concerned shall be informed about the follow-up given to the exercise of his rights of rectification and erasure as soon as possible and in any event not later than three months from the date on which he applies for rectification or erasure or sooner if national law so provides.	7. The person concerned shall be informed about the follow-up given to the exercise of his ***or her*** rights to rectification erasure ***and to restriction of processing*** as soon as possible and in any event not later than ***60 days*** from the date on which he ***or she*** applies for rectification***,*** or erasure ***or for a restriction of processing*** or sooner if national law so provides. ***The person shall be informed under this paragraph regardless of whether he or she is on Union territory or not.***	7. ~~The person concerned shall be informed about the follow up given to the exercise of his rights of rectification and erasure as soon as possible and in any event not later than three months from the date on which he applies for rectification or erasure or sooner if national law so provides.~~[171]	
828	*Article 66*	*Article 66*	*Article 66*	*Article 66*
829	*Remedies*	*Remedies*	*Remedies*	*Remedies*
830	1. Any person may bring an action before the courts or the authority competent under the law of any Member State to access, rectify, erase or obtain information	1. ***Without prejudice to Articles 77 to 82 of Regulation (EU) 2016/679 and Articles 52 to 56 of Directive (EU) 2016/680*** any person may bring an action before the courts or the authority	1. Any person may bring an action before the courts or **any competent** ~~the~~ authority ~~any competent authorities, including courts,~~ under the **national** law ~~of~~	

[170] Paragraph merged with paragraph 7.
[171] Merged with paragraph 6.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	or to obtain compensation in connection with an alert relating to him.	competent under the law of any Member State to access, rectify, erase information or to obtain ***a processing restriction and*** compensation in connection with an alert relating to him ***or her***.	~~any Member State~~ to access, rectify, erase or obtain information or to obtain compensation in connection with an alert relating to him.	
831	2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1 of this Article, without prejudice to the provisions of Article 70.		2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1 of this Article, without prejudice to the provisions of Article 70.	2. The Member States undertake mutually to enforce final decisions handed down by the courts or authorities referred to in paragraph 1 of this Article, without prejudice to the provisions of Article 70.
832	3. In order to gain a consistent overview of the functioning of remedies the national authorities shall develop a standard statistical system for reporting annually on:		3. ~~In order to gain a consistent overview of the functioning of remedies~~ **T**he national authorities shall ~~develop a standard statistical system for reporting~~**(…) report** annually on:	***Member States shall report annually on***: LIBE accepts the compromise proposal
833	(a) the number of subject access requests submitted to the data controller and the number of cases where access to the data was granted;		(a) the number of subject access requests submitted to the data controller and the number of cases where access to the data was granted;	(a) the number of subject access requests submitted to the data controller and the number of cases where access to the data was granted;
834	(b) the number of subject access requests submitted to the national supervisory authority and the number of		(b) the number of subject access requests submitted to the national supervisory authority and the number of	(b) the number of subject access requests submitted to the national supervisory authority and the number of

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	cases where access to the data was granted;		cases where access to the data was granted;	cases where access to the data was granted;
835	(c) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data to the data controller and the number of cases where the data were rectified or erased;	(c) the number of requests for the rectification of inaccurate data and the erasure ***or restriction of processing*** of unlawfully stored data to the data controller and the number of cases where the data were rectified or erased;	(c) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data to the data controller and the number of cases where the data were rectified or erased;	To be further discussed.
836	(d) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data submitted to the national supervisory authority;	(d) the number of requests for the rectification of inaccurate data and the erasure ***or restriction of processing*** of unlawfully stored data submitted to the national supervisory authority;	(d) the number of requests for the rectification of inaccurate data and the erasure of unlawfully stored data submitted to the national supervisory authority;	
837	(e) the number of cases which are heard before the courts;		(e) the number of cases **in which a final court decision was handed down**[172] ~~which are heard before the courts;~~	(e) the number of ***court proceedings launched*** ~~cases~~ **~~in~~** ~~which~~ **~~a final court decision was handed down~~** ~~are heard before the courts~~; LIBE does accept this text.
838	(f) the number of cases where the court ruled in favour of	(f) the number of cases where the court ruled in favour of the applicant in any aspect of the case ***and the number of cases where***	~~(f)~~[173] ~~the number of cases where the court ruled in favour of~~	

[172] Text from point (f).
[173] Merged with point (e).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	the applicant in any aspect of the case;	***compensation was obtained***;	~~the applicant in any aspect of the case~~; **and**	
839	(g) any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts created by the alert-issuing Member State.		(g) any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts created by the ~~**alert**~~ issuing Member State.	(g) any observations on cases of mutual recognition of final decisions handed down by the courts or authorities of other Member States on alerts created by the ~~**alert**~~ issuing Member State.
840	The reports from the national supervisory authorities shall be forwarded to the cooperation mechanism set out in Article 69.		The reports from the national supervisory authorities shall be forwarded to the cooperation mechanism set out in Article 69.	***A template for the reporting referred to in the first subparagraph shall be developed by the Commission. The reports from the ~~national supervisory authorities~~ Member States shall be forwarded to the European Data Protection Board established by Regulation (EU) 2016/679 and be included in the joint report referred to in Article 52(4).***
841	*Article 67*	*Article 67*	*Article 67*	*Article 67*
842	*Supervision of N.SIS*	*Supervision of N.SIS*	*Supervision of N.SIS*	*Supervision of N.SIS*
843	1. Each Member State shall ensure that the national supervisory authority(ies) designated in each Member State and endowed with the powers referred to in Chapter VI of Directive (EU) 2016/680 or	1. Each Member State shall ensure that the national ***independent*** supervisory ***authorities*** designated in each Member State and endowed with the powers referred to in Chapter	1. Each Member State shall ensure that the national supervisory authorit**y**~~(ies)~~ designated in each Member State and endowed with the powers referred to in Chapter VI of Directive (EU) 2016/680 or	LIBE compromise proposal: 1. Each Member State shall ensure that the independent national supervisory ***authorities*** designated in each Member State

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Chapter VI of Regulation (EU) 2016/679 monitor independently the lawfulness of the processing of SIS personal data on their territory and its transmission from their territory, and the exchange and further processing of supplementary information.	VI of Directive (EU) 2016/680 or Chapter VI of Regulation (EU) 2016/679 monitor independently the lawfulness of the processing of SIS personal data on their territory and its transmission from their territory, and the exchange and further processing of supplementary information.	Chapter VI of Regulation (EU) 2016/679 monitor independently the lawfulness of the processing of SIS personal data on their territory and its transmission from their territory, and the exchange and further processing of supplementary information **on their territory**.	and endowed with the powers referred to in Chapter VI of Directive (EU)2016/680 or Chapter VI of Regulation (EU) 2016/679 monitor ~~independently~~ the lawfulness of the processing of SIS personal data on their territory and its transmission from their territory, and the exchange and further processing of supplementary information **on their territory**.
844	2. The national supervisory authority shall ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit shall either be carried out by the national supervisory authority, or the national supervisory authority(ies) shall directly order the audit from an independent data protection auditor. The national supervisory authority shall at all times retain control over and undertake the responsibilities of the independent auditor.	2. The national supervisory ***authorities*** shall ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit shall either be carried out by the national supervisory ***authorities***, or the national supervisory ***authorities*** shall directly order the audit from an independent data protection auditor. The national supervisory ***authorities*** shall at all times retain control over and undertake the responsibilities of the independent auditor.	2. The national supervisory authority shall ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit shall either be carried out by the national supervisory authority, or the national supervisory authorit**y**~~(ies)~~ shall directly order the audit from an independent data protection auditor. The national supervisory authority shall at all times retain control over and undertake the responsibilities of the independent auditor.	2. The national supervisory ***authorities*** shall ensure that an audit of the data processing operations in its N.SIS is carried out in accordance with international auditing standards at least every four years. The audit shall either be carried out by the national supervisory ***authorities***, or the national supervisory ***authorities*** shall directly order the audit from an independent data protection auditor. The national supervisory ***authorities*** shall at all times retain control over and undertake the responsibilities of the independent auditor.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
845	3. Member States shall ensure that their national supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.	3. Member States shall ensure that their national supervisory ***authorities have*** sufficient resources to fulfil the tasks entrusted to ***them*** under this Regulation. ***They shall also ensure that their national supervisory authorities have access to assistance from persons with expertise on biometric data.***	3. Member States shall ensure that their national supervisory authority has sufficient resources to fulfil the tasks entrusted to it under this Regulation.	LIBE compromise proposal: (based on Art. 55(3) EES) 3. Member States shall ensure that their national supervisory ***authorities have*** sufficient resources to fulfil the tasks entrusted to ***them*** under this Regulation~~.~~ ***and have access to advice from persons with sufficient knowledge of biometric data.***
846	*Article 68*	*Article 68*	*Article 68*	*Article 68*
847	*Supervision of the Agency*	*Supervision of the Agency*	*Supervision of the Agency*	*Supervision of the Agency* Council expressed scepticism on the EP changes.
848	1. The European Data Protection Supervisor shall ensure that the personal data processing activities of the Agency are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.	1. The European Data Protection Supervisor shall shall ***be responsible for monitoring*** the personal data processing activities of the Agency, ***the European Border and Coast Guard, Europol and Eurojust and for ensuring that those activities*** are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.	1. The European Data Protection Supervisor shall ensure that the personal data processing activities of the Agency are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.	COM will prepare a proposal On the basis of COM's proposal the monitoring is already included in the respective articles (Articles 46 and Article 49).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
849	2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with international auditing standards at least every four years. A report on that audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.	2. The European Data Protection Supervisor shall ensure that an audit of the Agency's, ***the European Border and Coast Guard's, Europol's and Eurojust's*** personal data processing activities is carried out in accordance with international auditing standards at least every four years. A report on that audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.	2. The European Data Protection Supervisor shall ~~ensure that~~**carry out** an audit of the Agency's personal data processing activities ~~is carried out~~ in accordance with international auditing standards at least every four years. A report on that audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.	LIBE compromise proposal: 2. The European Data Protection Supervisor shall ~~ensure that~~ **carry out** an audit of the Agency's***, the European Border and Coast Guard Agency's and Europol's*** personal data processing activities ~~is carried out~~ in accordance with international auditing standards at least every four years. A report on that audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency***, the European Border and Coast Guard Agency and Europol*** shall be given an opportunity to make comments before the report is adopted.
850		***2a. The European Data Protection Supervisor shall be granted sufficient resources to fulfil the tasks entrusted to it under this Regulation, including assistance from persons with expertise on biometric data.***		LIBE compromise proposal: Provision may be included in recital 32a: ***The European Data Protection Supervisor should be granted sufficient resources to fulfil the tasks entrusted to it under this Regulation, including assistance***

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				from persons with expertise on biometric data.
851	*Article 69*	*Article 69*	*Article 69*	*Article 69*
852	*Cooperation between national supervisory authorities and the European Data Protection Supervisor*	*Cooperation between national supervisory authorities and the European Data Protection Supervisor*	*Cooperation between national supervisory authorities and the European Data Protection Supervisor*	*Cooperation between national supervisory authorities and the European Data Protection Supervisor*
853	1. The national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall actively cooperate within the framework of their responsibilities and shall ensure coordinated supervision of SIS.	1. The national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall actively cooperate ***with each other*** within the framework of their responsibilities ***in accordance with Article [62] of [New Regulation 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]***.	1. The national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall actively cooperate within the framework of their responsibilities and shall ensure coordinated supervision of SIS.	1. The national supervisory authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall actively cooperate within the framework of their responsibilities and shall ensure coordinated supervision of SIS.
854	2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties in the interpretation or application of this		2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties in the interpretation or application of this	2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties in the interpretation or application of this

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Regulation and other applicable legal acts of the Union, study problems that are revealed through the exercise of independent supervision or through the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.		Regulation and other applicable legal acts of the Union, study problems that are revealed through the exercise of independent supervision or through the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.	Regulation and other applicable legal acts of the Union, study problems that are revealed through the exercise of independent supervision or through the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.
855	3. For the purposes laid down in paragraph 2, the national supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year as part of the European Data Protection Board established by Regulation (EU) 2016/679. The costs and servicing of these meetings shall be borne by the Board established by Regulation (EU) 2016/679. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.		3. For the purposes laid down in paragraph 2, the national supervisory authorities and the European Data Protection Supervisor shall meet at least twice a year as part of the European Data Protection Board established by Regulation (EU) 2016/679. ~~The costs and servicing of these meetings shall be borne by the Board established by Regulation (EU) 2016/679.~~Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary.	LIBE does not agree with the Council's deletion. This part of the text is, for example, also included in EES.
856	4. A joint report of activities as regards coordinated supervision shall be sent by the Board established by Regulation (EU)		4. A joint report of activities as regards coordinated supervision shall be sent by the Board established by Regulation (EU)	4. A joint report of activities as regards coordinated supervision shall be sent ***annually*** by the Board established by Regulation (EU)

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	2016/679 to the European Parliament, the Council, and the Commission every two years.		2016/679 to the European Parliament, the Council, and the Commission ~~every two years~~**annually**.	2016/679 to the European Parliament, the Council, and the Commission.
857	**CHAPTER XVI**	**CHAPTER XVI**	**CHAPTER XVI**	**CHAPTER XVI**
858	**LIABILITY**	LIABILITY ***AND PENALTIES***	**LIABILITY AND PENALTIES**[174]	**LIABILITY AND PENALTIES**[175]
859	*Article 70*	*Article 70*	*Article 70*	*Article 70* Presidency compromise:
860	*Liability*	*Liability*	*Liability*	*Liability*
861	1. Each Member State shall be liable for any damage caused to a person through the use of N.SIS. This shall also apply to damage caused by the issuing Member State, where the latter entered factually inaccurate data or stored data unlawfully.	1. Each Member State ***and eu-LISA shall*** be liable for any ***material or immaterial*** damage caused to a person ***as a result of an unlawful processing operation, as a result of any act incompatible with this Regulation or*** through the use of N.SIS. This shall also apply to damage caused by the issuing Member State, where the latter entered factually inaccurate data or stored data unlawfully.	1. Each Member State shall be liable**, in accordance with the national law,** for any damage caused to a person through the use of N.SIS. This shall also apply to damage caused by the issuing Member State, where the latter entered factually inaccurate data or stored data unlawfully.	(deleted)
862		***1a. Any person who, or Member State which, has suffered material or immaterial damage as***		1. Any person or Member State that has suffered material or non-material damage as a result of

174 "And Penalties" has been added, due to the inclusion of new Article 53A / 70A.
175 "And Penalties" has been added, due to the inclusion of new Article 53A / 70A.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		a result of an unlawful processing operation or of any act incompatible with this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered or from eu-LISA if it is responsible for the damage suffered. The Member State or eu-LISA shall be partially or fully relieved of that liability if it proves that the harmful event cannot be attributed to it. Claims for compensation brought against a Member State shall be governed by the provisions of national law of the defendant Member State, in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680.		an unlawful processing operation or any other act incompatible with this Regulation shall be entitled to receive compensation from the Member State which is responsible for the damage suffered or from the Agency which is responsible for the damage suffered only where it has not complied with obligations of this Regulation specifically directed to it or where it has acted outside or contrary to lawful instructions of that Member State. That Member State or the Agency shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event which gave rise to the damage.
863	2. Where the Member State against which an action is brought is not the Member State issuing the alert, the latter shall be required to reimburse, on request, the sums paid out as compensation unless the use of data by the Member State requesting reimbursement infringes this Regulation.		2. Where the Member State against which an action is brought is not the Member State issuing the alert, the latter shall be required to reimburse, on request, the sums paid out as compensation unless the use of data by the Member State requesting reimbursement infringes this Regulation.	(deleted)

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
864	3. Where any failure by a Member State to comply with its obligations under this Regulation causes damage to SIS, that Member State shall be held liable for the damage, unless and in so far as the Agency or another Member States participating in SIS failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.		3. Where any failure by a Member State to comply with its obligations under this Regulation causes damage to SIS, that Member State shall be held liable for the damage, unless and in so far as the Agency or ~~another~~**other** Member States participating in SIS failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.	3. If any failure of a Member State to comply with its obligations under this Regulation causes damage to the SIS, that Member State or body shall be held liable for such damage, unless and insofar as the Agency or another Member State participating in the SIS failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.
865				3a. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 3 shall be governed by the national law of the defendant Member State. Claims for compensation against the Agency for the damage referred to in paragraphs 1 and 3 shall be subject to the conditions provided for in the Treaties.
866				[3b. The issuing Member State shall be required to reimburse to another Member State, on request, the sums paid out as compensation to a person by the latter Member State, unless the use of data by the

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				that Member State infringes this Regulation.]
		Article 70 a	***Article 70A***	***Article 70A***
867		***Penalties***	***Penalties***[176]	***Penalties***[177]
868		***Member States shall ensure that any processing of data stored in SIS or any exchange of supplementary information contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive and shall include administrative and criminal penalties.***	**Member States shall ensure that any misuse of data entered in SIS or any exchange of supplementary information contrary to this Regulation is subject to effective, proportionate and dissuasive penalties in accordance with national law.**	*Council will propose text*
869		***Europol and the European Border and Coast Guard Agency shall ensure that members of their staff or members of their teams accessing SIS under their authority who process data stored therein in breach of this Regulation are subject to sanctions by the Agency or, in the case of team members, by their home Member State.***		LIBE withdraws its amendment (deleted)

176 New Article, similar to Article 65 of Decision 2007/533/JHA.
177 New Article, similar to Article 65 of Decision 2007/533/JHA.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
870	**CHAPTER XVII**	**CHAPTER XVII**	**CHAPTER XVII**	**CHAPTER XVII**
871	**FINAL PROVISIONS**	**FINAL PROVISIONS**	**FINAL PROVISIONS**	**FINAL PROVISIONS**
872	*Article 71*	*Article 71*	*Article 71*	*Article 71*
873	*Monitoring and statistics*	*Monitoring and statistics*	*Monitoring and statistics*	*Monitoring and statistics*
874	1. The Agency shall ensure that procedures are in place to monitor the functioning of SIS against objectives, relating to output, cost-effectiveness, security and quality of service.		1. The Agency shall ensure that procedures are in place to monitor the functioning of SIS against objectives, relating to output, cost-effectiveness, security and quality of service.	1. The Agency shall ensure that procedures are in place to monitor the functioning of SIS against objectives, relating to output, cost-effectiveness, security and quality of service.
875	2. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in Central SIS.		2. For the purposes of technical maintenance, reporting**,** **data quality reporting** and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in Central SIS.	2. For the purposes of technical maintenance, reporting, **data quality reporting** and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in Central SIS.
876	3. The Agency shall produce, daily, monthly and annual statistics showing the number of records per category of alert, the annual number of hits per category of alert, how many times SIS was searched and how many times SIS was accessed for the purpose of	3. The Agency shall produce, daily, monthly and annual statistics showing the number of records per category of alert, the annual number of hits per category of alert, how many times SIS was searched and how many times SIS was accessed for the purpose of entering, ***completing,*** updating or	3. The Agency shall produce, daily, monthly and annual statistics showing the number of records per category of alert, **in total, and for each Member State. The Agency shall also provide reports on** the ~~annual~~ number of hits per category of alert, how many times SIS was	3. The Agency shall produce, daily, monthly and annual statistics showing the number of records per category of alert, **in total, and for each Member State. The Agency shall also provide annual reports on** the ~~annual~~ number of hits per category of alert, how many times

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	entering, updating or deleting an alert in total and for each Member State. The statistics produced shall not contain any personal data. The annual statistical report shall be published. The Agency shall also provide annual statistics on the use of the functionality on making an alert issued under pursuant to Article 26 of this Regulation temporarily non-searchable, in total and for each Member State, including any extensions to the retention period of 48 hours.	deleting an alert in total and for each Member State. The statistics produced shall not contain any personal data. The annual statistical report shall be published. The Agency shall also provide annual statistics on the use of the functionality on making an alert issued pursuant to Article 26 of this Regulation temporarily non-searchable, in total and for each Member State, including any extensions to the retention period of 48 hours.	searched and how many times SIS was accessed for the purpose of entering, updating or deleting an alert**,** in total and for each Member State. The statistics produced shall not contain any personal data. The annual statistical report shall be published. The Agency shall also provide annual statistics on the use of the functionality on making an alert issued ~~under~~ pursuant to Article 26 of this Regulation temporarily non-searchable, in total and for each Member State, including any extensions to the ~~retention~~**initial non-searchable** period of 48 hours.	SIS was searched and how many times SIS was accessed for the purpose of entering, updating or deleting an alert**,** in total and for each Member State, including statistics on the consultation procedure referred to in Article 26. The statistics produced shall not contain any personal data. The annual statistical report shall be published.
877	4. Member States as well as Europol, Eurojust and the European Border and Coast Guard Agency shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraphs 3, 7 and 8. This information shall include separate statistics on the number of searches carried out by, or on behalf of, by the services in the Member States responsible for	4. Member States as well as Europol, Eurojust and the European Border and Coast Guard Agency shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraphs 3, 7 and 8. This information shall include separate statistics on the number of searches carried out by the ***competent authorities*** in the Member States responsible for	4. Member States as well as Europol, Eurojust and the European Border and Coast Guard Agency shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraphs 3, **5,** 7 and 8[178]**.**	4. Member States as well as Europol, Eurojust and the European Border and Coast Guard Agency shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraphs 3, **5,** 7 and 8[179]**.**

178 Text moved to paragraph 4a.
179 Text moved to paragraph 4a.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	issuing vehicle registration certificates and the services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines; aircraft and containers. The statistics shall also show the number of hits per category of alert.	issuing vehicle registration certificates and the ***competent authorities*** in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines; aircraft and containers. The statistics shall also show the number of hits per category of alert.		
878			**4a.**[180] This information shall include separate statistics on the number of searches carried out by, or on behalf of, ~~by~~ the services in the Member States responsible for issuing vehicle registration certificates and the services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines~~;~~ **,** **and** aircraft**, including aircraft engines** ~~and containers~~. The statistics shall also show the number of hits per category of alert.	**4a.**[181] This information shall include separate statistics on the number of searches carried out by, or on behalf of, ~~by~~ the services in the Member States responsible for issuing vehicle registration certificates and the services in the Member States responsible for issuing registration certificates or ensuring traffic management for boats, including boat engines~~;~~ **,** **and** aircraft**, including aircraft engines** ~~and containers~~. The statistics shall also show the number of hits per category of alert.
879	5. The Agency shall provide the Member States, the	5. The Agency shall provide the ***European Parliament, the***	5. The Agency shall provide the Member States, the	Council maintains its position; strong reservation in particular

[180] Moved from paragraph 4.
[181] Moved from paragraph 4.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	Commission, Europol, Eurojust and the European Border and Coast Guard Agency with any statistical reports that it produces. In order to monitor the implementation of legal acts of the Union, the Commission shall be able to request the Agency to provide additional specific statistical reports, either regular or ad hoc, on the performance or use of SIS and SIRENE communication.	***Council, the*** Member States, the Commission, Europol, ***Eurojust*** and the European Border and Coast Guard Agency ***and the European Data Protection Supervisor*** with any statistical reports that it produces ***and any specific statistical reports requested***. In order to monitor the implementation of legal acts of the Union, the Commission shall be able to request the Agency to provide additional specific statistical reports, either regular or ad-hoc, on the performance or use of SIS and SIRENE communication.	Commission, Europol, Eurojust and the European Border and Coast Guard Agency with any statistical reports that it produces. In order to monitor the implementation of legal acts of the Union, **in particular the Council Regulation (EU) No 1053/2013**[182]**,** the Commission shall be able to request the Agency to provide additional specific statistical reports, either regular or ad-hoc, on the performance or use of **Central** SIS and ~~SIRENE communication~~**on the exchange of supplementary information.**	regarding the production of "specific statistical reports". To be further discussed.
880	6. For the purpose of paragraphs 3, 4 and 5 of this Article and of Article 15(5), the Agency shall 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	6. For the purpose of paragraphs 3, 4 and 5 of this Article and of Article 15(5), the Agency shall 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	6. For the purpose of paragraphs 3, 4 ~~and~~**or** 5 of this Article and of Article 15(5), the Agency shall establish, implement and host a central repository in its technical sites containing the ~~data~~**reports** referred to in paragraph 3 of this Article and in Article 15(5) which shall not allow for the identification of individuals	LIBE proposal: 6. For the purpose of paragraphs 3***, 4 and*** 5 of this Article and ***of*** Article 15(5), the Agency shall 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

[182] 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).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	shall allow the Commission and the agencies referred to in paragraph 5 to obtain bespoke reports and statistics. The Agency shall grant access to Member States, the Commission, Europol, Eurojust and the European Border and Coast Guard Agency 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.	the agencies referred to in paragraph 5 to obtain bespoke reports and statistics. ***Upon request, the*** Agency shall grant access to Member States, the Commission, Europol, Eurojust and the European Border and Coast Guard Agency to the central repository ***specific items and information*** 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.	and shall allow the Commission and the agencies referred to in paragraph 5 to obtain bespoke reports and statistics. The Agency shall grant access to Member States, the Commission, Europol, Eurojust and the European Border and Coast Guard Agency 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.	identification of individuals and shall allow the Commission and the agencies referred to in paragraph 5 to obtain bespoke reports and statistics. ***Upon request, the*** Agency shall ***give*** access to Member States, the Commission, Europol, ~~***Eurojust***~~ and the European Border and Coast Guard Agency to the central repository~~***, specific items and information***~~ 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.
881	Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be adopted by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).	Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be adopted by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).	~~Detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository shall be adopted by means of implementing measures adopted in accordance with the examination procedure referred to in Article 72(2).~~[183]	
882	7. Two years after SIS is brought into operation and every two years thereafter, the Agency	7. ***One year*** after SIS is brought into operation and every two years thereafter, the Agency shall submit to the European	7. ~~Two years after SIS is brought into operation and~~ **E**very two years ~~thereafter,~~ the Agency	LIBE proposal: 7. Two years after SIS is brought into operation and every two years

[183] Moved to paragraph 9.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.	Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof ***on the functioning of the automated fingerprint identification system***, and the bilateral and multilateral exchange of supplementary information between Member States.	shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, and the bilateral and multilateral exchange of supplementary information between Member States.	thereafter, the Agency shall submit to the European Parliament and the Council a report on the technical functioning of Central SIS and the Communication Infrastructure, including the security thereof, ***on the introduction of the automated fingerprint identification system*** and the bilateral and multilateral exchange of supplementary information between Member States. ***This report shall also contain, once the technology is in use, an evaluation of the use of facial images to identify a third-country national.***
883	8. Three years after SIS is brought into operation and every four years thereafter, the Commission shall produce an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in	8. ***One year*** after SIS is brought into operation and every ***two*** years thereafter, the Commission shall produce an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation ***shall take the opinion of the European Data Protection Supervisor into account, and*** shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale,	8. ~~Three years after SIS is brought into operation and~~ **E**very four years ~~thereafter,~~ the Commission shall produce an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation shall include an examination of results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in	Council maintains its position and finds the 1-year premature and the 2 years too frequent. LIBE proposal: 8. Three years after SIS is brought into operation and every four years thereafter, the Commission shall produce an overall evaluation of Central SIS and the bilateral and multilateral exchange of supplementary information between Member States. That overall evaluation shall include an examination of

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
	respect of Central SIS, the security of Central SIS and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council.	the application of this Regulation in respect of Central SIS, the security of Central SIS and any implications for future operations. ***The overall evaluation report shall also include the creation of an automated fingerprint file function and SIS information campaigns organised by the Commission in accordance with Article 19.*** The Commission shall transmit the evaluation to the European Parliament and the Council.	respect of Central SIS, the security of Central SIS and any implications for future operations. The Commission shall transmit the evaluation to the European Parliament and the Council.	results achieved against objectives, and an assessment of the continuing validity of the underlying rationale, the application of this Regulation in respect of Central SIS, the security of Central SIS and any implications for future operations. ***The overall evaluation report shall also include an assessment of the automated fingerprint identification system and SIS information campaigns organised by the Commission in accordance with Article 19.*** The Commission shall transmit the evaluation to the European Parliament and the Council.
884			**9.**[184] **The Commission shall adopt implementing acts to lay down and develop** detailed rules on the operation of the central repository **referred to in paragraph 6** and security rules applicable to **that repository. Those** implementing **acts shall be** adopted in accordance with the examination procedure referred to in Article 72(2).	LIBE proposal: **9. The Commission shall adopt implementing acts to lay down ~~and develop~~** detailed rules on the operation of the central repository **referred to in paragraph 6** and the data protection and security rules applicable to ~~the~~ **that** repository ~~shall be laid down and developed by means of~~**. Those** implementing ~~measures~~ **acts shall be** adopted in

[184] Text moved from paragraph 6, *in fine*.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
				accordance with the examination procedure referred to in Article 72(2).
885		***Article 71 a***		
886		***Exercise of the delegation***		
887		***1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.***		To be updated once overall agreement is reached. Where necessary for a specific delegation of power, an urgency provision could be added.
888		***2. The power to adopt delegated acts referred to in Article 8(4), Article 12(7), Article 22 (-1), Article 42(4), Article 51(3) and Article 75(2a) shall be conferred on the Commission for an indeterminate period of time from ... [the date of entry into force of this Regulation].***		
889		***3. The delegation of power referred to in Article 8(4), Article 12(7), Article 22 (-1), Article 42(4), Article 51(3) and Article 75(2a) 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***		

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.		
890		***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 of 13 April 2016 on Better Law-Making.***		
891		***5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.***		
892		***6. A delegated act adopted pursuant to Article 8(4), Article 12(7), Article 22 (-1), Article 42(4), Article 51(3) and Article 75(2a) 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***		

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
		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.		
893	*Article 72*	*Article 72*	*Article 72*	*Article 72*
894	*Committee procedure*	*Committee procedure*	*Committee procedure*	*Committee procedure*
895	1. The Commission shall be assisted by a committee within the meaning of Regulation (EU) No 182/2011.		1. The Commission shall be assisted by a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by a committee within the meaning of Regulation (EU) No 182/2011.
896	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.
897	*Article 73*		*Article 73*	
898	*Amendments to Regulation (EU) 515/2014*		~~Amendments to Regulation (EU) 515/2014~~	

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
899	Regulation (EU) 515/2014[185] is amended as follows:		~~Regulation (EU) 515/2014[186] is amended as follows:~~	
900	In Article 6, the following paragraph 6 is inserted:		~~In Article 6, the following paragraph 6 is inserted:~~	
901	"6. During the development phase Member States shall receive an additional allocation of 36,8 million EUR to be distributed via a lump sum to their basic allocation and shall entirely devote this funding to SIS national systems to ensure their quick and effective upgrading in line with the implementation of Central SIS as required in Regulation (EU) 2018/…* and in Regulation (EU) 2018/…**		~~"6. During the development phase Member States shall receive an additional allocation of 36,8 million EUR to be distributed via a lump sum to their basic allocation and shall entirely devote this funding to SIS national systems to ensure their quick and effective upgrading in line with the implementation of Central SIS as required in Regulation (EU) 2018/…* and in Regulation (EU) 2018/…**~~	
902	**Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police and judicial cooperation for criminal matters and in Regulation (OJ…..*		~~**Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police and judicial cooperation for criminal matters and in Regulation (OJ…..*~~	

185 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 (OJ L 150, 20.5.2014, p. 143).

186 ~~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 (OJ L 150, 20.5.2014, p. 143).~~

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
903	***Regulation (EU 2018/…on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and in Regulation (OJ …)".*		~~***Regulation (EU 2018/…on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and in Regulation (OJ …)".*~~[187]	
904	*Article 74*		*Article 74*	*Article 74*
905	*Repeal*		*Repeal*	*Repeal*
906	Upon the date of application of this Regulation the following legal acts are repealed:		Upon the date of application of this Regulation the following legal acts are repealed:	Upon the date of application of this Regulation the following legal acts are repealed:
907	Regulation (EC) No 1986/2006 of 20 December 2006 of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates;		Regulation (EC) No 1986/2006 of 20 December 2006 of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates;	Regulation (EC) No 1986/2006 of 20 December 2006 of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates;
908	Council Decision 533/2007/JHA of 12 July 2007 on the establishment, operation and use of the second generation Schengen Information System (SISII);		Council Decision ~~533/~~2007/**533**/JHA of 12 July 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II);	Council Decision ~~533/~~2007/**533**/JHA of 12 July 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II);

187 Article removed, as this instrument does not amend Regulation (EU) 515/2014.

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
909	Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure[188].		Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure[189].	Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure[190].
910	*Article 75*	*Article 75*	*Article 75*	*Article 75*
911	*Entry into force and applicability*	*Entry into force and applicability*	*Entry into force and applicability*	*Entry into force and applicability*
912	1. This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.		1. This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.	1. This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.
913	2. It shall apply from the date fixed by the Commission after:	2. It shall apply from ***[one year after the date of entry into force] with the exception of Article 5, Article 8(4), Article 9(1), Article 12(7), Article 15(5) and (6), Article 20(3) and (4), Article 22(-1), Article 32(5) and (7), Article 34(3), Article 36(5), Article 38(3), Article 42(4), Article 51(3), Article 59(4), Article 60(6), Article 71(6) and Article 75(2a), which shall apply from the date of entry into force of this Regulation.***	2. It shall apply from the date fixed by the Commission after:	

188 Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (OJ L 112, 5.5.2010, p.31).
189 Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (OJ L 112, 5.5.2010, p. 31).
190 Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (OJ L 112, 5.5.2010, p. 31).

	COM PROPOSAL (15814/16)	PARLIAMENT	COUNCIL (14116/17)	COMPROMISE
914	(a) the necessary implementing measures have been adopted;	***deleted***	(a) the necessary implementing measures have been adopted;	
915	(b) Member States have notified the Commission about that they have made the necessary technical and legal arrangements to process SIS data and exchange supplementary information pursuant to this Regulation;	***deleted***	(b) Member States have notified the Commission ~~about~~ that they have made the necessary technical and legal arrangements to process SIS data and exchange supplementary information pursuant to this Regulation;	
916	(c) The Agency has notified the Commission about the completion of all testing activities with regard CS-SIS and the interaction between CS-SIS and N.SIS.	***deleted***	(c) The Agency has notified the Commission ~~about~~**of** the **successful** completion of all testing activities with regard **to** CS-SIS and the interaction between CS-SIS and N.SIS.	
917		***2a. The Commission shall be empowered to adopt delegated acts in accordance with Article 71a concerning amendments to the date of application of this Regulation.***		
918	3. This Regulation shall be binding in its entirety and directly applicable to Member States in accordance with the Treaty on the Functioning of the European Union.		~~3.~~ This Regulation shall be binding in its entirety and directly applicable to Member States in accordance with the Treat**ies**~~y on the Functioning of the European Union~~.	LIBE proposal (based on standard wording) ~~3.~~ This Regulation shall be binding in its entirety and directly applicable ***in the*** ~~to~~ Member States in accordance with the Treat**ies**~~y on the Functioning of the European Union~~.
