COUNCIL OF THE EUROPEAN UNION

Brussels, 13 January 2006

5318/06

LIMITE

SIRIS 10
SCHENGEN 3
COMIX 45

NOTE

from :	Presidency
to :	Schengen Acquis Working Party (Mixed Committee EU/Iceland, Norway and Switzerland)
Subject :	Draft Council Decision on SIS II Articles 15-48

1. Following discussions in the Schengen Acquis working party in July to December 2005, the Presidency has produced this consolidated text of Articles 15 – 48 of the draft Council Decision on the SIS II including footnotes and making textual proposals where appropriate.

2. The consolidated text is attached as in Annex A.

ARTICLES 15–48 OF THE PROPOSAL FOR A COUNCIL DECISION ON THE ESTABLISHMENT, OPERATION AND USE OF THE SECOND GENERATION SCHENGEN INFORMATION SYSTEM II (SIS II)

CHAPTER IV

Alerts in respect of persons wanted for arrest and surrender or extradition

Article 15

Objectives and conditions for issuing alerts

Alerts shall be issued in the SIS II at the request of the competent judicial authority in respect of persons wanted for arrest and surrender on the basis of a European Arrest Warrant or in respect of persons wanted for provisional arrest with a view to extradition.

*Article 1**6 (ex Article 17)***

*Additional data on persons wanted for arrest **with a view to surrender or** extradition*

1. In addition to the alert referred to in Article 15, the issuing Member State shall enter into the SIS II the following data on persons wanted for arrest and **surrender or** extradition:
   (a) the identity and nationality of the wanted person;
   (b) **[**the name, address, telephone and fax numbers and e-mail address of the**]**[1] **the** issuing judicial authority;
   (c) **reference to** an enforceable judgment or any other enforceable judicial decision having the same effect;
   (d) the nature and legal classification of the offence;
   (e) a description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the wanted person;

[1] The Presidency includes this recognising that given the information is to be contained in the SIS II itself it may not be necessary to include the name, address, telephone and fax numbers and email address. The Presidency would ask delegations if this detail should be deleted accordingly. DE would prefer the text in square brackets to remain included in the substantive text.

(f) the penalty imposed, if there is a final judgment, or the prescribed scale of penalties for the offence under the law of the issuing Member State;

(g) if possible, other consequences of the offence.

2. The issuing Member State may enter a translation of the additional data referred to in paragraph 1 in one or more other official languages of the institutions of the European Union.[2]

Article 17 ***(ex Article 16)***

Additional data on persons wanted for arrest ***(…) with a view to*** *surrender*

1. If a person is wanted for arrest and surrender on the basis of a European Arrest Warrant, in addition to the alert referred to in Article 15, the issuing Member State shall enter into the SIS II **(…)** a copy of the original of the European Arrest Warrant[3].

2. The issuing Member State may enter a translation of the data referred to in paragraph 1 and/or of the original of the European Arrest Warrant in one or more other official languages of the institutions of the European Union.

Article 18

Authorities with right to access to alerts and additional data on persons wanted for arrest

1. The following authorities shall[4] have the right to access the alerts referred to in Article 15, for the purposes specified:
   (a) police**, (…)** border **and customs** authorities[5], for the purposes of arrest;
   (b) national judicial authorities and those responsible for public prosecutions, for the purpose of criminal proceedings.[6] [7]
2. The European Police Office (Europol) shall have the right to access the data contained in alerts for arrest which is necessary for the performance of its tasks in accordance with the Convention of 26 July 1995 on the establishment of a European Police Office ("the Europol Convention").

---

2 DE would want the data referred to in paragraph (2) to be considered as coded (language-free) data and to be recorded in free text only in exceptional circumstances.

3 PT and EL queried why if an alert constitutes an EAW and all the necessary information is included why a copy of the EAW was also necessary.

4 The Presidency notes that some delegations would prefer not to make the right to access mandatory.

5 The Presidency notes that at least one delegation would prefer to extend the list to cover circumstances in which a court may make an arrest.

6 AT suggests this phrase should read "National judicial authorities and authorities responsible for public prosecutions as well as their co-ordinating authorities for the purpose of criminal proceedings."

7 DE entered a scrutiny reservation.

3. Eurojust shall have the right to access the data contained in alerts for arrest and the data referred in Articles 16 and 17 which is necessary for the performance of its tasks in accordance with Decision 2002/187/JHA.

4. National judicial authorities and those responsible for public prosecutions shall have the right to access the data referred to in Article**s** 16 **and 17** for the purpose of executing a European Arrest Warrant and the data referred to in Article **16** for the purpose of the extradition procedure.

Article 19

Conservation period of the alerts and additional data for arrest

1. Alerts **referred to in Article 15** and the additional data referred to in Articles 16 and 17 shall be kept in the SIS II until the wanted person has been surrendered or extradited. They shall only be kept for as long as the issuing Member State considers the warrant valid according to its national law.

2. Alerts issued for arrest and the additional data referred to in Articles 16 and 17 shall automatically be erased after 10 [8] years **from the date the alert was entered in the SIS II**[9]. The Member State having entered the data in the SIS II may decide to keep it in the system, should this prove necessary for the purpose for which the data was entered.

3. Member States will be informed **automatically four months** before the automatic erasure of the data from the system.

Article 20

Flagging related to alerts on persons wanted for arrest ***with a view to surrender or extradition***

1. When a flag has been added to an alert **referred to in Article 15 (…)** in accordance with Article 45 and the arrest cannot be made but the location of the person is known to the Member State which added the flag**, the Member State which added the flag** shall **(…) communicate the place of residence or domicile of the person to the Member State issuing the alert by the exchange of supplementary information**.

[8] Some delegations queried the extension of time for which data could be held.
[9] The Presidency suggests this is the easiest moment to count the period of retention of data from.

2. The need for maintaining a flag added to an alert **referred to in Article 15 (…)** shall be reviewed at least every **(…) year** by the Member State adding the flag. Member States may provide for a shorter review period.[10]

Article 21

Flagging related to alerts for arrest and surrender

1. **Where Framework Decision 2002/548/JHA applies, a** flag as provided for in Article 45 (1) prohibiting arrest may only be added to an alert for arrest and surrender where the competent judicial authority[11] **of the executing Member State** has given authorisation on the basis of a **(…)** ground for the non-execution of a European Arrest Warrant based on Framework Decision 2002/548/JHA or where the person has been provisionally released following arrest.[12]

   (…)

2. The prohibition on arrest and surrender shall remain effective until the flag is erased.

   A flag shall be erased as soon as the grounds for non-execution of the European Arrest Warrant have ceased to exist or the provisional release has ended.

3. **(…)**

Article 22

Execution of action based on an alert on a person wanted for arrest ***(…) with a view to*** *surrender* ***or extradition***

1. An alert entered in the SIS II **referred to in Article 15 in combination with the additional data referred to in Articles 16 and 17 (…)** shall **constitute[13] and have the same effect in terms of the action to be taken as (…)** a European Arrest Warrant issued in accordance with Article 9 (3) of Framework Decision 2002/584/JHA.

---

[10] DE scrutiny reserve.

[11] DE would prefer to broaden the term and to replace it with the phrase "competent authorities under national law."

[12] There was no consensus as to which MS should add the flag though DE would prefer it to be added by the State issuing the alert at the request of another State.

[13] The Presidency would note that this phrasing implies that the data referred to in Articles 16 and 17 would be enough to constitute an EAW (i.e. no further documentation or communication with the issuing Member State would be needed).

2. Where Framework Decision 2002/548/JHA does not apply, an alert referred to in Article 15 I combination with the additional data referred to in Article 16 shall have the same force as a request for provisional arrest under Article 16 of the European Convention on Extradition of 13 September 1957 or Article 15 of the Benelux Treaty[14] concerning Extradition and Mutual Assistance in Criminal Matters of 27 June 1962, as amended by the Protocol of 11 May 1974 and shall have the same effect as regards the action to be taken.

Chapter V

Alerts on missing persons to ensure protection or prevent threats [15]

Article 23[16][17]

Objectives and conditions for issuing alerts

1. Member States shall issue in the SIS II alerts on missing persons or persons who, for their own protection or in order to prevent threats, need to be placed under temporary (…) protection[18] at the request of the competent administrative or judicial authority.
2. Alerts referred to in paragraph 1 shall be issued in particular with respect to missing minors and persons who must be interned following a decision by a competent authority.

[14] The Presidency would ask Member States and the Benelux Member States in particular whether such a reference in this provision, which is taken from the current text of the Schengen Implementing Convention, is still necessary for SIS II.

[15] BE suggested "missing" be reinserted in the title.

[16] ES and DK prefer the wording of Article 97 SIC.

[17] JSA notes that Art 24 introduces a separate objective of communicating the whereabouts of the missing person, which needs to be combined with the objective in Art 23 of placing the individual under temporary protection – these two objectives need to be combined.

[18] Some delegations (NL, DE, FR, CY, PT) requested the term "police" be removed.

Article 24

Authorities with right to access to alerts

1. Police and border authorities[19] shall have the right to access the alerts referred to in Article 23 for the purpose of putting the person concerned under (…) protection[20] or for the purpose of tracing[21] the whereabouts of a missing person.[22]
2. National judicial authorities[23], *inter alia* those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 23, in the performance of their tasks.[24]

Article 25

Conservation period of the alerts

1. Alerts issued for the purpose of ensuring protection or preventing threats shall be erased as soon as the person is placed under police protection.
2. The alerts referred to in paragraph 1 shall automatically be erased after 10 years[25] from **the date the alert was entered in the SIS II**[26]. The Member State having entered the alert in the SIS II may decide to keep the alert in the system, should this prove necessary for the purpose for which the alert was entered.
3. Member States will be informed **automatically four** month**s** before the automatic erasure of the alerts from the system.

---

[19] CZ, FR, BE would like to include customs. PT would like a reference to civil authorities and BE suggests that Article 101 of SIC is used as an alternative approach.

[20] See earlier reference to "police protection"

[21] The Presidency notes that "tracing" is used here. It may be better to use consistent terms to describe the action to be taken throughout this chapter.

[22] FR question why Eurojust would not have access. The Commission noted that under the current terms of the SIS, Eurojust would not have access to the equivalent of this data.

[23] SE and MT would prefer a reference to competent authorities.

[24] AT suggests this phrase should read "National judicial authorities and authorities responsible for public prosecutions as well as their co-ordinating authorities for the purpose of criminal proceedings."

[25] Some MS and JSA/EDPS query why a 10 year conservation period has been proposed by the Commission.

[26] Delegations suggested this should refer to the date of entry of the alert. The Presidency suggests that it is the approach that should be taken horizontally throughout the text where this issue arises.

Article 26

Execution of action based on an alert

1. The competent authorities of the Member State where a person referred to in Article 23 is found shall communicate the whereabouts of the person to the Member State issuing the alert by the exchange of supplementary information.

   The detailed rules for this exchange shall be adopted in accordance with Article 61 and inserted in the SIRENE Manual.

2. The communication of the whereabouts of a missing person who is of age shall be subject to that person's consent.

3. The competent authorities of the Member State where a person referred to in Article 23 is found may move the person to a safe place[27] in order to prevent that person from continuing his journey, if so authorised by national law.[28]

Chapter VI

Alerts on persons who are sought so as to be able to assist with a judicial procedure[29]

Article 27

Objectives and conditions for issuing alerts

[30]At the request of a *competent national authority*, Member States shall issue in the SIS II alerts on[31]:

- **witnesses,**
- **persons who are to be served with a writ, a summons, a decision or equivalent information within the framework of criminal proceedings,**

---

27 PT would like "safe place" clarified

28 DE scrutiny reserve.

29 CZ would prefer an alternative term in place of "wanted" given it may suggest the person is being sought by the police for criminal reasons. So the Presidency has suggested the chapter be retitled: "Alerts on persons who are sought so as to be able to assist with a judicial procedure" as above.

30 Changes made following the suggestion of SE and DK.

31 FI would also suggest that alerts should be entered on persons who are searched to be summoned to appear before national judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted.

- **persons summoned to appear before the national judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted,**
- **persons who are to be served with a criminal judgement,**
- **persons who are to be served with a summons to report in order to serve a penalty involving deprivation of liberty,**

for the purpose of communicating their place of residence or domicile.[32] [33]

Article 28

Authorities with right to access to alerts

1. Police and border authorities[34][35] shall have the right to access the alerts referred to in Article 27 for the purpose of ascertaining the place of residence or domicile of the persons concerned.
2. National judicial authorities, *inter alia* those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 27 which are necessary for the performance of their tasks.
3. Eurojust shall have the right to access the data contained in alerts referred to in Article 27 which are necessary for the performance of its tasks in accordance with Decision 2002/187/JHA.

Article 29

Conservation period of alerts

1. Alerts referred to in Article 27 shall be erased as soon as the place of residence or domicile of the person concerned has been ascertained.[36]
2. Alerts referred to in Article 27 shall automatically be erased after 10 years from the date **the alert was entered in the SIS II** [37]. The Member State having entered the alert in the SIS II may decide to keep the alert in the system, should this prove necessary for the purpose for which the alert was entered.

---

[32] Change made following the suggestion of SE and DK.
[33] FI wanted to clarify that domicile should include the concept of a persons' whereabouts.
[34] SE suggest replacing "police" with "law enforcement authorities"
[35] CZ, DE, FR and AT would like "customs" to be included. ES would like this to be clarified by adding "where pursuant to national legislation".
[36] FR suggested retaining the alerts beyond the moment when the place of residence has been obtained and until the judicial authority has completed its task. NL supports this approach.
[37] Delegations suggested this should refer to the date of entry of the alert. The Presidency suggests that it is the approach that should be taken horizontally throughout the text where this issue arises.

3. Member States will be informed **automatically four** month**s** before the automatic erasure of the alerts from the system.

Article 30

Execution of the action based on an alert

1. The competent authorities of the Member State where a person referred to in Article 27 is found shall communicate the place of residence or domicile of the person to the Member State issuing the alert by the exchange of supplementary information.
2. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

Chapter VII

Alerts on persons and objects for discreet surveillance[38] or specific checks

Article 31

Objectives and conditions for issuing alerts

1. At the request of the competent judicial or administrative authority[39], Member States shall, for the purposes of prosecuting criminal offences and for the prevention of threats to public security, issue in the SIS II alerts on persons or vehicles, boats, aircrafts and containers[40] for the purpose of discreet surveillance or of specific checks[41] in the following circumstances:

---

[38] Several delegations felt surveillance did not accurately represent the activity that happened. LU suggested the alert should be described as *"discrete checks"*. FR and NO supported this interpretation. IT disagreed saying the term "surveillance" was most appropriate. The Presidency suggests that surveillance would best describe the situation in Article 40 of the Schengen Convention where a person is being observed for a prolonged period of time but is unaware he is being observed. The term *"discrete checks"* would better describe a situation in which a person was approached by a police officer and that person was aware that he had been *"checked"* by the police and his identity had been confirmed. Should delegations agree that the action to be taken would require or allow the police officer to approach the person in question, the Presidency suggests *"discrete checks"* would be a better term to use. The rest of the Article should be amended to reflect that action.

[39] DE, PT, AT, EL would like a reference to police added. The Presidency would suggest the phrase could read "administrative authority, including police authorities, …"

[40] Delegations were divided as to whether it was possible to hold checks on objects without them being linked to persons, SL suggested that objects and people were always linked, EL, BE and LU disagreed.

[41] A number of delegations noted that paragraph 1 refers to "objects" but paragraphs (a) and (b) refer to the circumstances in which *"surveillance"* of persons only is carried out. Delegations queried whether it would be helpful to add additional sub-clauses setting out the circumstances in which checks on objects may be carried out too or to make clear that the objects referred to are objects that have been involved in the committing of "serious criminal offences".

(a) where there is clear evidence[42] that the person concerned intends to commit or is committing (…)[43] an extremely serious criminal offence[44] or

(b) where an overall assessment of the person concerned, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit extremely serious criminal offences in the future.

2. Member States may issue alerts in the SIS II, at the request of the authorities responsible for national security, where there is clear evidence that the information referred to in Article 32 is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security.[45] The Member State issuing the alert shall inform the other Member States thereof by the exchange of supplementary information. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61[46] and inserted in the SIRENE Manual.

Article 32

Collection and exchange of supplementary information for alerts

1. In cases of alerts for discreet surveillance, the competent authorities of the Member States which carry out border checks or other police and customs checks within the country may collect and communicate to the authority issuing the alert all or some of the following information:

(a) the fact that the person for whom, or the vehicle for which an alert has been issued has been found;

(b) the place, time or reason for the check;

(c) the route and destination of the journey;

(d) the persons accompanying the persons concerned or the occupants of the vehicle[47];

---

42 NO suggest replacing "clear evidence" with "reason to believe". LT, DE, LU supported this.

43 The Presidency deleted the word "numerous" considering that one serious offence should be sufficient.

44 NO considers "serious criminal offence" should be defined by reference to the offences in the EAW. SE, CZ support this. FR opposes. LU support definition alternative could be the Europol. FI support common view.

45 FR suggests this alert is removed as so few alerts had been entered. DE, AT, NL, BE disagreed and preferred to retain it.

46 ES did not think this should be left to comitology and that Council should be authorised to make such decisions referring the CLS to the appropriate ECJ judgement (Case C-257/01) which supported their position. EL supported.

47 NO suggests this provisions should specifically include boats and aircrafts.

(e) the vehicle used;

(f) objects carried[48];

(g) the circumstances under which the person or the vehicle was found.

2. The information referred to in paragraph 1 shall be communicated by the exchange of supplementary information. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

3. For the collection of the information referred to in paragraph 1, Member States shall take the necessary steps not to jeopardise the discreet nature of the surveillance.

4. During the specific checks referred to in Article 31, persons, vehicles, boats, aircraft, containers and objects carried may be searched in accordance with national law for the purposes referred to in that Article. If specific checks are not authorised under the law of a Member State, they shall automatically be replaced, in that Member State, by discreet surveillance.

Article 33

Authorities with right to access to alerts

1. Police, border and customs authorities shall have the right to access to the alerts referred to in Article 31 for the purpose of performing discreet surveillance or specific checks.

2. National judicial authorities[49], inter alia those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 31 in the performance of their tasks.[50]

3. Europol shall have the right to access to the data of the alerts referred to in Article 31 which are necessary to perform its tasks in accordance with the Europol Convention.

---

[48] LT suggested this provision does not apply to discreet surveillance only to the performance of a detailed search. The Presidency would link this concern to the wider concern of what "surveillance" means and what action should be taken under this alert.

[49] DE also wanted the police to have access.

[50] AT suggests this phrase should read "National judicial authorities and authorities responsible for public prosecutions as well as their co-ordinating authorities for the purpose of criminal proceedings."

Article 34

Conservation period of alerts

1. Alerts on persons issued pursuant to Article 31 shall automatically be erased after 3 years[51] from **the date of entry of the alert in the SIS II**.
2. Alerts on objects issued pursuant to Article 31 shall automatically be erased after 5 years from **the date of entry of the alert in the SIS II**.
3. The Member State having entered an alert in the system may decide to keep the alert in the SIS II, should this prove necessary for the purpose for which the alert was entered.
4. Member States will be informed **automatically four months** before the automatic erasure of the alerts from the system.

Chapter VIII

Alerts on objects for seizure or use as evidence in criminal proceedings[52]

Article 35[53]

Objectives and conditions for issuing alerts

1. At the request of the competent authority, Member States shall, for the purposes of seizure or use as evidence in criminal proceedings, issue in the SIS II alerts on the following objects[54]:
   (a) motor vehicles with a cylinder capacity exceeding 50cc, boats and aircrafts[55] which have been stolen, misappropriated or lost;
   (b) trailers with an unladen weight exceeding 750 kg, caravans, industrial equipment, outboard engines and containers which have been stolen, misappropriated or lost;
   (c) firearms[56] which have been stolen, misappropriated or lost;
   (d) blank official documents which have been stolen, misappropriated or lost;

[51] NO thought a 1 year retention period was more proportionate. SE and DK agreed.
[52] LT, LV and NO considered the scope of this article too limited. They found that alerts on objects should also include other objects (for instance objects related to an offence) than stolen, misappropriated, lost or for seizure or use as evidence in criminal proceedings.
[53] CZ, DE, ES and NO would prefer the wording of Art. 100 SIC. ES entered a reserve of principle.
[54] AT, BE and DE felt that the expression «readily identifiable» should be inserted, like in the Spanish Initiatives.
[55] HU would prefer *registered crafts, boats and aircrafts* or another wider terminology instead of *firearms*.
[56] HU would prefer *objects and technologies qualified as arms*.

(e) issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated[57];

(f) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated;

(g) banknotes (registered notes)[58];

(h) securities and means of payment such as cheques, credit cards, bonds, stocks and shares which have been stolen, misappropriated or lost[59].

2. [60]The Commission shall establish the technical rules necessary for entering and accessing the data contained in the alerts referred to in paragraph 1 in accordance with Article 60.[61]

Article 36

Collection and exchange of supplementary information for alerts

1. If a search[62] brings to light an alert for an object which has been found, the authority[63] of the Member State where the object was found shall contact[64] the authority which issued the alert, in order to agree on the[65] measures to be taken. For this purpose, personal data may be communicated in accordance with this Decision.

2. [66]The contacts and communication of personal data referred to in paragraph 1 shall be done through the exchange of supplementary information. The detailed rules for this exchange shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

3. The measures to be taken by the Member State which finds the object shall be in accordance with its national law.

---

57 SE expressed doubts on the action to be taken following a hit on an invalidated passport.
58 HU would prefer *banknotes (registered notes) which are object of a criminal act*.
59 SE would prefer *stolen, misappropriated, lost or invalidated*.
60 FR entered a reservation on comitology.
61 The Presidency indicated that though access for vehicle registration authorities should be governed by the terms of draft Regulation XX/05 of the Commission, the categories of data to which they may have access should be more clearly defined in the draft Council Decision itself. The Presidency thought this would respond to the concern of NO relating to the possibility that vehicle registration authorities would be given wider access than was necessary for them to fulfil their purpose.
62 BE noted a possible translation problem in the French version. It could accept "*interrogation*", not "*recherche*".
63 CZ, FR and LV would prefer *SIRENE bureaux* instead of *authorities*.
64 FR and LV considered that in certain cases there is no need for such a contact, for instance in case of a stolen document.
65 COM proposed the replacement of *the* with *further*.
66 ES and FR entered a reservation.

Article 37[67]

Authorities with right to access to alerts[68] [69] [70] [71]

1. Police, border and custom authorities shall have the right to access the alerts referred to in Article 35 for the purpose of seizure of the object.
2. National judicial authorities, inter alia those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, may have access to the alerts referred to in Article 35, in the performance of their tasks.[72]
3. Europol shall have the right to access the data contained in the alerts referred to in Article 35 which are necessary to perform its tasks, in accordance with the Europol Convention.

Article 38[73]

Conservation period of alerts[74]

1. Alerts on objects referred to in Article 35 shall be erased as soon as the objects have been seized.[75]
2. Alerts referred to in Article 35 which contain no personal data shall automatically be erased after a period of ten years from **the date the alert was entered in the SIS II**.
3. [76]Alerts referred to in Article 35 which contain personal data shall automatically be erased in the SIS II after a period of three years[77] **from the date the alert was entered in the SIS II**.
4. The Member State having entered the alert in the SIS II may decide to keep the alert in the system for a period longer than the conservation periods laid down in paragraphs 2 and 3 should this prove necessary for the purpose for which the alerts were entered.
5. Member States will be informed **automatically four months** before the automatic erasure of the alerts from the system.

---

67 ES and FR suggested the replacement of this article with a text similar to Art. 101 SIC.
68 AT wondered whether this provision should also cover the coordination between authorities.
69 CH would prefer more authorities, for instance in relation to firearms. ES noted that a wider range of authorities under national law should have access to the data on these alerts.
70 BE, DE and EL considered that Eurojust should also have access.
71 HU thought that immigration authorities should also have access to data related to documents.
72 AT suggests this phrase should read "National judicial authorities and authorities responsible for public prosecutions as well as their co-ordinating authorities for the purpose of criminal proceedings."
73 FR entered a scrutiny reservation on this article.
74 DE suggested to keep current periods and practices.
75 BE, ES and LV expressed some concerns about the seizure of vehicles. BE stressed that in practice, alerts on cars are erased only after they are back to their country.
76 FI would prefer the current SIC text.
77 NO asked for more than three years for documents.

CHAPTER IX

General data processing rules

Article 39

Categories of data

1. No more than the following data shall be contained in the alerts on persons issued in the SIS II in application of this Decision[78]:
   (a) surname(s) and forename(s), name at birth and previously used names and any aliases, possibly entered separately;
   (b) date and place of birth;
   (c) sex;
   (d) photographs;
   (e) fingerprints;
   (f) nationality;
   (g) any specific objective and physical characteristics not subject to (…)[79] change;
   (h) whether the person concerned is armed, violent or has escaped;
   (i) reason for the alert;
   (j) authority issuing the alert[80];
   (k) action to be taken;
   (l) in cases of alerts for arrest, the type of offence;
   (m) link(s) to other alerts processed in the SIS II.
2. The data referred to in paragraph 1 shall only be used for the purpose of identifying[81] a person in view of a specific action to be taken in accordance with this Decision.[82]
3. The Commission shall establish the technical rules necessary for entering and accessing the data referred to in paragraph 1 in accordance with Article 61[83].

---

78 Clarification needed on whether this is mandatory

79 DE suggested deletion of "frequent". The JSA would like justification for the use of this term "frequent". The Presidency has consequently deleted the term.

80 LT, DK, CZ did not want this included in the list as they questioned its usefulness and thought it may lead to some authorities choosing not to issue or use alerts. The JSA does not think this information is relevant. COM supported by ES notes that a similar provision need not be included in the Draft Regulation on SIS II.

81 DK noted that identifying was substantially different to verifying. DE did not think identification was adequate because this alerts cover additional issues such as ensuring the safety of police officers carrying out the checks.

82 LU suggests that this reference be deleted as it appears superfluous. ES supported this.

83 FR did not support the use of comitology in this context.

Article 40[84]

Processing of SIS II data

1. Data entered in the SIS II pursuant to this Decision shall only be processed for the purposes and by the competent national authorities defined by the Member States in accordance with this Decision.
2. [85]A Member State may change the category of an alert to another only if this is necessary to prevent an imminent serious threat to public policy, public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence. The alert whose category is changed shall be considered as a new alert issued by the Member State requesting the change of category. For this purpose a prior authorisation of the Member State that issued the first alert shall be obtained by the exchange of supplementary information. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61[86] and inserted in the SIRENE Manual.
3. Access to SIS II data shall only be authorised within the limits of the competence of the national authority and to duly authorised staff.
4. Each Member State shall maintain and transmit to the Commission an up-to-date list[87] of national authorities who are authorised to process SIS II data. That list shall specify, for each authority, which category of data it may process, for what purpose and who is to be considered as controller[88], and shall be communicated by the Commission to the European Data Protection Supervisor. The Commission shall ensure the annual publication of the list in the *Official Journal of the European Union*.

---

84 ES would prefer a text similar to Art. 102(3) and 101 SIC to replace Articles 40(2) and 40(3) respectively.

85 Most delegations (BE, DE, EL, ES, FR LV, NO and SE) expressed concerns on this paragraph and wondered whether it was necessary. The Presidency notes that the relationship between Article 40(2) and (3) needed to be clarified. COM was invited to redraft this paragraph in a more clear way.

86 ES entered a reservation concerning the use of comitology. The Presidency noted that the application of comitology to the Third Pillar was a matter for Coreper to consider but that the more the substantive text was clear on the action to be taken etc. the less there was a need for any implementing rules at all.

87 AT, EL, ES and FR expressed concerns about the confidentiality of this list. They do not agree with the creation of new obligations on this matter. They considered that such list should also be transmitted to the Council.

88 Some delegations asked for more clarity concerning this concept.

Article 41[89]

Entering a reference number

(…)

Article 42

Copy of SIS II data

1. Except for the copy of data of the CS-SIS referred to in Article 4 (3), the data processed in the SIS II may only be copied for technical purposes and provided that such copying is necessary for the competent national authorities to access the data in accordance with this Decision.
2. Data entered into the SIS II by another Member State shall not be copied into Member State's own national data files.[90]
3. Paragraph 2 shall not prejudice the right of a Member State to keep in its national file SIS II data in connection with which action has been taken on its territory.[91] Such data shall be kept in national files for a maximum period of three years[92], except if specific provisions in national law provide for a longer retention period.
4. This article shall not prejudice the right of a Member State to keep in its national files data contained in a particular alert, which that Member State has issued in the SIS II.

Article 43

Quality of the data processed in the SIS II and compatibility between alerts

1. [93]The Member State entering the data in the SIS II shall be responsible for ensuring that that data is processed lawfully and, in particular, that it is accurate and up-to-date.
2. Only the Member State which entered data in the SIS II shall modify, add to, correct or erase it.

---

89 The Working Party agreed in principle on the deletion of this article.

90 SE noted that Article 42(2) could be read to mean that a Member State could not copy its own data into its own national files.

91 BE wondered how this provision could work in practise. COM was asked to clarify the text.

92 SE and NO would prefer to keep the text of the Spanish Initiatives.

93 ES and DK entered a reservation on this paragraph as it seemed impossible to make the issuing Member State responsible for further processing of data that occurred in another Member State.
COM was invited to rephrase this paragraph in accordance with the current text of Article 105 SIC.

3. [94]If a Member State, which did not enter the data, has evidence suggesting that data is incorrect or has been unlawfully processed in the SIS II, it shall inform the Member States[95] which entered the data by exchanging supplementary information at the earliest opportunity and if possible not later then 10 days after the evidence comes to its attention. The Member State which entered the data shall check it and, if necessary, modify, add to, correct or erase it. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

4. If Member States are unable to reach agreement within two months about the correction of the data, any of them may[96] submit the case to the European Data Protection Supervisor who shall act as mediator.

5. [97]The Member States shall exchange supplementary information in order to distinguish accurately between alerts in the SIS II related to persons with similar characteristics. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

6. [39]When a person is already the subject of an alert in the SIS II, the Member State issuing a new alert in respect of the same person shall reach agreement on the entry of this new alert with the Member State which issued the first alert. The agreement shall be reached on the basis of the exchange of supplementary information. The detailed rules for this exchange of supplementary information shall be adopted in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual.

   Different alerts on the same person may be entered in the SIS II if they are compatible[98]. The rules governing the compatibility of and priority of categories of alerts shall be determined in accordance with the procedure set out in Article 61.

7. Data kept in the SIS II shall be reviewed at least annually[99] by the issuing Member State. Member States may provide for a shorter review period.

---

[94] DE, ES and LV considered this text not clear and that this provision could provoke some delays. LV suggested that the text be clear that where a disagreement arose that could not be resolved, the older alert would be considered the valid alert.

[95] DK noted this word should read "State".

[96] ES, FI, FR and HU would prefer replacing *may* with *shall*.

[97] ES preferred no comitology.

[98] DK requested clarification of the term "compatible" and what that would mean in practice. The Presidency noted that rule could either be set out in the text of the legal instruments or handled separately in the comitology process.

[99] Many delegations (CZ, DE, FI, FR, LV, NO and SE) opposed to an annual review. DK suggested a horizontal approach was needed throughout the text to the periods for which data was retained. The Presidency noted that a balance was needed between a proposal to delete the annual review of data which would be disproportionate and unworkable and the length of time for which data could be retained and renewed.

Article 44

Additional data for the purpose of dealing with misidentifications of persons[100]

1. [101]**The data related to an individual whose identity has been misused shall only be added with that individual's explicit consent and shall only be used for the following purposes**[102]**:**
   (a) **to allow the competent authority to differentiate the individual whose identity has been misused from the person actually intended by the alert;**
   (b) **to allow the individual whose identity has been misused to prove his identity and to establish that his identity has been misused.**
2. **Where confusion may arise between the person actually intended by an alert and a person whose identity has been misused, Member States shall add data related to the latter to the alert in order to avoid the negative consequences of misidentifications.**
3. No more than the following personal data may be entered and further processed in SIS II for the purpose of this article:
   (a) surname(s) and forename(s), any aliases[103] possibly entered separately;
   (b) date and place of birth;
   (c) sex;
   (d) photographs;
   (e) fingerprints;
   (f) any specific objective and physical characteristic not subject to frequent change;
   (g) nationality;
   (h) number(s) of identity paper(s)[104] and date of issuing.
4. The data referred to in paragraph 3 shall be erased at the same time as the corresponding alert or earlier if the person so requests.
5. Only the authorities having the right to access the corresponding alert may access the data referred to in paragraph 3 and for the sole purpose of avoiding misidentification.
6. The technical rules referred to in Article 39 (3) shall apply to the data referred to in paragraph 3 of this article.

---

[100] BE suggested the insertion of other biometric data than photographs and fingerprints.
[101] Paragraphs 1 and 2 have been reordered at the suggestion of FI.
[102] FR invited COM to rephrase this paragraph in a more clear way so that it covered, as the Presidency agreed it should, persons whose identity had been misused deliberately by another person (stolen) and persons who were simply misidentified (by mistake).
[103] CZ noted that misidentification would not apply to aliases.
[104] CZ suggested to draft this paragraph in accordance with the rules of Data Dictionary.

Article 45[105]

Flagging

1. A Member State may add a flag to the alerts issued in accordance with Articles 15, 23 and 31 to the effect that the action to be taken on the basis of the alert will not be taken on its territory.

   A flag may be added to an alert where a Member State considers that an alert issued in the SIS II is incompatible with its national law, its international obligations or essential national interests.

2. **(…)**

3. A Member State wishing to add a flag to an alert shall consult the Member State issuing the alert by the exchange of supplementary information. The detailed rules for that exchange shall be defined in accordance with the procedure defined in Article 61 and inserted in the SIRENE Manual. If the Member State issuing the alert does not withdraw the alert, it shall continue to apply in full to Member States which do not add a flag.

4. **(…)**

5. **(…)**[106]

6. The procedure and technical rules for adding flags and updating them shall be adopted in accordance with Article 60.

[105] DE notes that it should be the State that entered the alert that enters the flag at the request of another Member State.
[106] DE wants to keep this paragraph as in particularly urgent and serious cases the issuing Member State should be able to demand that a flag be reviewed.

Article 46[107][108]

Links between alerts

1. A Member State may create a link between alerts it issues in the SIS II in accordance with its national legislation. The effect of such a link shall be to establish a relationship between two or more alerts.[109]
2. The creation of a link shall not affect the specific action to be taken[110] on the basis of each linked alert or the conservation period of each of the linked alerts.
3. The creation of links shall not affect the rights to access provided for in this Decision. Authorities with no right to access certain categories of alerts shall not have access to the links to those categories.
4. When a Member State considers that the creation 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.
5. The technical rules for linking alerts shall be adopted in accordance with Article 60[111].

Article 47[112]

Purpose and conservation period of supplementary information

1. The supplementary information transmitted by another Member State shall be used only for the purpose for which it was transmitted. It shall only be kept in national files as long as the alert to which it relates is kept in the SIS II. Member States may keep this information for a longer period if necessary to achieve the purpose for which it was transmitted[113]. In any event, the supplementary information shall be erased at the latest one year after the related alert has been erased from the SIS II.

---

[107] COM would submit a revised text of this article, more specific, indicating which alerts could be linked, how much links could concern an alert and under which situations a link could be make.

[108] DE supported the use of links and noted that linking between national alerts had worked well in practice in DE for some time. The Presidency noted that a compromise may lie in considering the maximum number of alerts that could be linked, the limitations on the actions that may be taken, and including clarity on who could see linked alerts. The effect of such a compromise would assist in making clear the burden placed on Member States and officers on the ground when alerts are introduced.

[109] NO commented that including links between alerts would begin the change of SIS II from being a hit/no-hit system to becoming an investigation system.

[110] AT, BE, CZ, DK, FR, NO thought there should be requirements for linking, without changing the purpose of the system (hit/no hit). These delegations considered that the creation of a link could affect the action to be taken. LV wondered about the effectiveness of this article.

[111] NO would prefer 61.

[112] COM was invited to present a clearer text.
HU suggested a better articulation between Articles 42 and 47.

[113] AT considered this provision not necessary.

2. Paragraph 1 shall not prejudice the right of a Member State to keep in national files data relating to a particular alert in connection with which action has been taken on its territory. Such data may be held in national files for a maximum period of three years[114], except if specific provisions of national law authorise retention of the data for a longer period.

Article 48

Transfer of personal data to third parties

1. Except if explicitly provided for in EU law[115], the **(…)** [116] data processed in the SIS II in application of this Decision shall not be transferred or made available to a third country or to an international organisation.
2. By way of derogation from paragraph 1, **(…)** data may be transferred[117] to third countries or international organisations in the framework of a European Union agreement in the field of police[118] or judicial cooperation guaranteeing an adequate level of protection of the transferred personal data and with the consent of the Member State that entered the data in the SIS II.

---

[114] ES and NO did not agree with this provision.
[115] NO suggested to replace *EU law* with *Schengen relevant provisions.*
[116] BE, DE, ES and NO suggested deleting "*personal"*.
[117] FR wondered whether this transfer was mutual and suggested to use *exchange* instead of *transfer.*
[118] SE suggested that the term "law enforcement" should be used in place of "police".