COUNCIL OF THE EUROPEAN UNION

Brussels, 27 January 2006

5709/06

Interinstitutional File: 2005/0106 (COD)

LIMITE

SIRIS 22
SCHENGEN 10
CODEC 71
COMIX 86

NOTE

from :	Presidency
to :	Schengen Acquis Working Party (Mixed Committee EU/Iceland, Norway and Switzerland)
No. prev. doc. :	9943/05 SIRIS 61 SCHENGEN 11 CODEC 486 COMIX 384 11760/05 SIRIS 81 SCHENGEN 23 COMIX 534 13134/05 SIRIS 101 SCHENGEN 31 COMIX 652 14498/1/01 SIRIS 125 SCHENGEN 41 COMIX 768 REV 1
Subject :	Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) - Redrafted proposal

Following discussion in the Schengen Acquis Working Party since July 2005, and taking into account the delegation's comments, the Austrian Presidency presents in the Annex a redrafted compromise version of the abovementioned proposal.

ANNEX

DRAFT COUNCIL REGULATION ON THE ESTABLISHMENT, OPERATION AND USE OF THE SECOND GENERATION SCHENGEN INFORMATION SYSTEM (SIS II)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Article 62 (2) (a) and Article 66 thereof,

CHAPTER I
General provisions

Article 1
Establishment and general objective of the SIS II

1. The European Community shall set up and maintain an information system, the second generation Schengen Information System (hereinafter referred to as "SIS II").
2. The purpose of the SIS II shall be, in accordance with this Regulation, to maintain public policy and public security, including national security, in the territories of the Member States and to apply the provisions of Title IV of the Treaty establishing the European Community (hereinafter referred to as "EC Treaty") relating to the movement of persons in their territories, using information communicated via this system.

Article 2
Scope

1. This Regulation defines the conditions and procedures for the processing of alerts issued in respect of third country nationals in the SIS II, and the exchange of supplementary information for the purpose of refusing entry into the territory of the Member States.

2. This Regulation also lays down provisions on the technical architecture of the SIS II, responsibilities, of the Member States and of the Management Authority referred to in Article 12, general data processing, rights of individuals concerned and liability.

Article 3

Definitions

1. For the purposes of this Regulation, the following definitions shall apply:

"alert" means a set of data entered in the SIS II allowing the competent authorities to identify a person or an object in view of a specific action to be taken;

"supplementary information" means the information not stored in the SIS II, but connected to SIS II alerts, which shall be exchanged in order to allow Member States to consult or inform each other whilst entering an alert, following a hit, when the required action cannot be taken, when dealing with the quality of SIS II data and when dealing with the compatibility of alerts as well as the exercise of the right of access;

"additional data" means the data stored in the SIS II and connected to SIS II alerts which shall be immediately available to the competent authorities where persons in respect of whom data has been entered in the SIS II are found as a result of searches made therein;

"third country national" means any individual who is not a citizen of the European Union within the meaning of Article 17 (1) of the EC Treaty and who is not a person enjoying the Community right of free movement;

"persons enjoying the Community right of free movement" means:

citizens of the Union within the meaning of Article 17 (1) of the EC Treaty, and third-country nationals who are members of the family of a citizen of the Union exercising his or her right to free movement, to whom Directive 2004/38/EC of the European Parliament and of the Council on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States [1] applies;

[1] OJ L 158, 30.04.04, p. 77.

third-country nationals and their family members, whatever their nationality, who, under agreements between the Community and its Member States, on the one hand, and the countries of which they are nationals, on the other, enjoy rights of free movement equivalent to those of citizens of the Union.

2. "Processing of personal data", "processing", and "personal data" shall be understood in accordance with Article 2 of Directive 95/46/EC of the European Parliament and of the Council[2].

[3]Article 4

Technical architecture and ways of operating the SIS II

1. The SIS II is composed of:
   (a) a national section (hereinafter referred to as "NS-SIS") in each of the Member States;
   (b) a central system (hereinafter referred to as "the Central SIS II") composed of:
      – a technical support function (hereinafter referred to as "CS-SIS") containing the reference database for SIS II;
      – a uniform national interface (hereinafter referred to as "NI-SIS");
   (c) a communication infrastructure between the CS-SIS and the NI-SIS (hereinafter referred to as "Communication Infrastructure") on a network dedicated to SIS II data.
2. SIS II data shall be searched via the NS-SIS. A NS-SIS may contain a data file (hereinafter referred to as "national copy"), containing a complete or partial copy from the reference database for SIS II. A national copy shall be available for the purposes of carrying out automated searches in the territory of each of the Member States. It shall not be possible to search the data files of other Member States' NS-SIS.
3. The principal central system of the CS-SIS, which carries out technical supervision and administration, is located in Strasbourg (France) and a backup central system, capable of ensuring all functionalities of the principal central system in case of failure of this system, is located in Sankt Johann in Pongau (Austria).

---

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

[3] JSA comments that it is not clear whether Member States may choose to process all SIS II alerts in a national copy of the CS-SIS or to have direct access to the CS-SIS. The JSA comments this choice may affect compliance with other provisions in the Decision such as the logging of processing and supervision.

4. The CS-SIS will provide the services necessary for the update of, and the searches in, the reference database for SIS II. For the Member States which use a national copy the CS-SIS will provide:

   the on-line update of the national copies;

   the synchronisation and the coherence between the national copies and the reference database for SIS II;

   the operation for initialisation and restoration of the national copies.

Article 5

Costs

1. The costs incurred in connection with the operation and maintenance of the Central SIS II and the Communication Infrastructure shall be borne by the budget of the European Union.
2. These costs will include work done with respect to the CS-SIS that ensures the synchronisation and the coherence between the national copies and the reference database for SIS II, including the operation for initialisation and restoration of the national copies.
3. The costs of developing, adapting and operating each NS-SIS shall be borne by the Member State concerned.
4. Additional costs incurred as a result of the use of the copies referred to in Article 4 (2) shall be borne by the Member States that make use of such copies.

CHAPTER II

Responsibilities of the Member States

[4]Article 6

National Systems

Each Member State, for its own account and at its own risk, shall:

(a) set up and maintain its NS-SIS;

(b) connect its NS-SIS to the NI-SIS.

[5]Article 7

SIS II national office[6] and SIRENE Bureau

1. (a) Each Member State shall designate an authority (hereinafter referred to as "SIS II national office"), which shall have central responsibility for its NS-SIS;

   (b) Each Member State shall issue its alerts via that authority;

   (c) The said authority shall be responsible for the smooth operation of the NS-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.

2. (a) Each Member State shall designate the authority which shall ensure the exchange of all supplementary information (hereinafter referred to as the "SIRENE Bureau");

   (b) This Bureau shall also coordinate the verification of the quality of the information entered into the SIS II;

   (c) For both purposes it shall have access to data processed in the SIS II.

3. The Member States shall inform each other and the Management Authority referred to in Article 12 of their SIS II national office and of their SIRENE Bureau.

---

4 JSA comments that there ought to be a specific provision defining what is meant by a national copy and the difference between it and a national system. The JSA suggests there be some way of recording the number of copies given to consulates. COM has commented that copies given to consulates are technical copies, there will only be one national copy.

5 The JSA notes that the lack of one central authority responsible for the national section of the SIS II may create serious problems in maintaining the national copy, data quality, control and supervision. See JSA comments on page 22 of the English version of 2501/05 SCHAC 1.

6 EL would prefer this to read "N.SIS II Office and Sirene Bureau."

Article 8

Exchange of supplementary information

1. Supplementary information shall be exchanged in accordance with national legislation and using the Communication Infrastructure.
2. Such information shall be used only for the purpose for which it was transmitted.
3. Should the Communication Infrastructure be unavailable, Member States may use other technical means for exchanging supplementary information.

Article 9

Technical Compliance

1. To ensure the rapid and effective transmission of data, each Member State shall observe, when setting up its NS-SIS, the protocols and procedures established for that purpose.
2. If a Member State uses a national copy it shall, by means of the CS-SIS, ensure that its national copy remains materially identical to the national copies of other Member States and to the reference database for SIS II.

Article 10

Security and confidentiality

1. Each Member State shall, in relation to its NS-SIS, adopt the necessary measures in order to:
   (a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);
   (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
   (c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
   (d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control).

2. Each Member State shall take special measures to ensure the security of data while they are being communicated to services located outside the territories of the Member States. Such measures shall be notified to the joint supervisory authority referred to in Article 31 (3).

3. For the processing of data in its NS-SIS each Member State may appoint only specially qualified persons who have undergone security checks.[7]

Article 11

Keeping of logs at national level

1. Each Member State shall ensure that every transmission of personal data is recorded in the NS-SIS for the purposes of checking whether the search is admissible or not, for the purpose of monitoring the lawfulness of data processing, ensuring the proper functioning of the NS-SIS, data integrity and security.

2. The records may only be used for this purpose and shall be deleted at the earliest after a period of one year and at the latest after a period of three years.

[7] BE suggests the following redraft: *"Each Member State shall apply his rules of professional secrecy or other equivalent obligations of confidentiality to all persons and bodies required to work with SIS II data and supplementary information, according his national legislation. This obligation shall also apply after those people leave office or employment or after the termination of the activities of those bodies"*.

Chapter III

Responsibilities of the authority responsible for the operational management of the Central SIS II and the Communication Infrastructure

Article 12

[8]Operational management

1. The Council of the European Union acting unanimously[9] shall designate the authority (hereinafter referred to as "the Management Authority") responsible for the operational management of the Central SIS II and the Communication Infrastructure. During the period preceding the final implementation of this Regulation, the French Republic and the Republic of Austria shall take charge of the operational management of the Central SIS II and the Communication Infrastructure.
2. The operational management shall consist of all the tasks necessary to keep the Central SIS II and Communication Infrastructure functioning on a 24 hours a day, 7 days a week basis in accordance with this Regulation, in particular the maintenance work and technical adaptations necessary for the smooth running of the system.

Article 13

Security and confidentiality

1. The Management Authority shall, in relation to the Central SIS II and the Communication Infrastructure, adopt the necessary measures in order to:

   deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

---

8 EL would prefer to add "Development and Operational management."

9 The Legal Service has doubts as to whether:
a) this is a matter that can be the subject of the exercise of implementing powers;
b) unanimity can be foreseen on this point.

prevent the unauthorised reading, copying, modification or removal of data media (data media control);

prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control).

2. The Management Authority shall take measures equivalent to those referred to in paragraph 1 as regards security and confidentiality in respect of the exchange of supplementary information through the communication infrastructure referred to in Article 4 (1)(c).

Article 14

Keeping of logs at central level

The Management Authority shall ensure that every transmission of personal data is recorded for the purposes provided for in Article 11 (1).

Article 14 A (former Article 16)

Categories of data

1. Without prejudice to Article 8 (1), the SIS II shall contain only those categories of data which are supplied by each of the Member States, as required for the purposes laid down in Article 15. The Member State issuing an alert shall determine whether the case is important enough to warrant entry of the alert in the SIS II.

2. The information on the persons for whom an alert has been issued shall be no more than the following:

surname(s) and forename(s), name at birth and previously used names and any aliases possibly entered separately;

any specific, objective, physical characteristics not subject to change;

place and date of birth;

sex;

photographs;

fingerprints;

nationality;

whether the persons concerned are armed, violent or have escaped;[10]

reason for the alert;[11]

authority issuing the alert;

a reference to the decision giving rise to the alert;

action to be taken;

link(s) to other alerts (…) issued in the SIS II.[12]

3. Other information, in particular the data listed in the first sentence of Article 6 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, shall not be authorised.

---

[10] Some delegations suggested adding "have escaped" and some felt the term "dangerous" was vague, others felt it to be unnecessary. DE placed a reserve on the term "dangerous" and preferred using the terms "armed, violent or has escaped".

[11] LU suggested that the field containing the reason for the alert and action to be taken should be combined.

[12] NO and DK underlined they would not accept links between all alerts in the SIS II.

Chapter IV

Alerts issued in respect of third country nationals for the purpose of refusing entry

[13]Article 15

Objectives and conditions for issuing alerts

1. Data on third country nationals for whom an alert has been issued for the purposes of refusing entry shall be entered on the basis of a national alert resulting from decisions taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law.
2. Decisions may be based on a threat to public policy or public security or to national security which the presence of a third country national in national territory may pose. This situation may arise in particular in the case of:

   a third country national who has been convicted of an offence carrying a penalty involving deprivation of liberty of at least one year;

   a third country national in respect of whom there are serious[14] grounds for believing that he has committed serious criminal offences, including those referred to in Article 2 (2) of Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States, or in respect of whom there is clear evidence of an intention to commit such offences in the territory of a Member State;

   a third country national who is the object of a restrictive measure intended to prevent entry into or transit through the territory of Member States, taken in accordance with Article 15 of the EU Treaty and/or a travel ban issued by the Security Council of the United Nations.

---

[13] DK suggested an additional subparagraph be added concerning the right/obligation to enter an alert for persons denied asylum under the terms of Article 1(f) of the UN Convention on Refugees.

[14] A number of delegations entered reserves on the use of the inclusion of the word "serious" and preferred it to be deleted. The Presidency kept this term in regard of the current text of Article 96 SIC.

3. Decisions may also be based on the fact that the third country national has been subject to measures involving deportation, refusal of entry or removal which have not been rescinded or suspended, including or accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of third country nationals.

Article 16

Categories of data

(...)

Article 17

Authorities with right to access the alerts[15]

1. Access to data entered in the SIS II and the right to search such data directly or in a copy of data of the CS-SIS shall be reserved exclusively to the authorities responsible for:
   (a) border checks;
   (b) other police and customs checks carried out within the country, and the coordination of such checks.
2. However, access to data entered in the SIS II and the right to search such data directly may also be exercised by national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation.
3. In addition, access to data entered in accordance with Article 15 and the data concerning documents relating to persons entered in accordance with Article 35 (3)(d) and (e) of Council Decision 2006/XX and the right to search such data directly may be exercised by the authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation on third country nationals in the context of the application of the Community acquis relating to the movement of persons. Access to data by these authorities shall be governed by the national law of each Member State.
4. Users may only search data which they require for the performance of their tasks.

[15] BE would like a reference to access to SIS II for Schengen Evaluation teams for the purposes of conducting evaluations. The Presidency indicated in the Schengen Evaluation working group that BE should produce a paper further motivating and explaining the need for this new access.

Article 18

Other authorities with right to access

(...)

Article 18 A

(...)

Article 19

Access to alerts on identity documents

(...)

Article 20

Conservation period of the alerts

1. Personal data entered into the SIS II for the pursuant to this Regulation shall be kept only for the time required to meet the purposes for which they were supplied. The Member State which issued the alert must review the need for continued storage of such data not later than three years after they were entered.
2. Each Member State shall, where appropriate, set shorter review periods in accordance with its national law.
3. The CS-SIS shall automatically inform the Member States of scheduled deletion of data from the system four months in advance.
4. The Member State issuing the alert may, within the review period, decide to keep the alert should this prove necessary for the purposes for which the alert was issued. Any extension of the alert must be communicated to the CS-SIS. The provisions of paragraph 1 shall apply to the extended alert.

CHAPTER V

General data processing rules

Article 21

Processing of SIS II data

1. The Member States may use the data provided for in Article 15 for the purposes of refusing entry to, or removal from, their territories.
2. Data may only be copied for technical purposes, provided that such copying is necessary in order for the authorities referred to in Article 17 to carry out a direct search. Alerts issued by other Member States may not be copied from the NS-SIS into other national data files.
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. Data entered under Article 15 and data concerning documents relating to persons entered under Article 35 (3)(d) and (e) of Council Decision xx/xxxx may be used in accordance with the national law of each Member State for the purposes referred to in Article 17 (3).
5. Any use of data which does not comply with paragraphs 1 to 4 shall be considered as misuse under the national law of each Member State.
6. Each Member State shall send the Management Authority a list of competent authorities which are authorised to search the data contained in the SIS II directly pursuant to this Regulation. That list shall specify, for each authority, which data it may search and for what purposes.

Article 22

Entering a reference number

(...)

Article 23

SIS II data and national files

1. Article 21 (1) shall not prejudice the right of a Member State to keep in its national files SIS II 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.
2. Article 21 (1) and Article 21 (2) 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 23 A

1. Alerts shall be governed by the national law of the Member State issuing the alert unless more stringent conditions are laid down in this Regulation.
2. Insofar as this Regulation does not lay down specific provisions, the law of each Member State shall apply to data entered in its NS-SIS.
3. In so far as this Regulation does not lay down specific provisions concerning performance of the action requested in the alert, the national law of the requested Member State performing the action shall apply. Insofar as this Regulation lays down specific provisions concerning performance of the action requested in the alert, responsibility for that action shall be governed by the national law of the requested Member State. If the requested action cannot be performed, the requested Member State shall immediately inform the Member State issuing the alert.

Article 24

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

1. The Member State issuing the alert shall be responsible for ensuring that the data entered into the SIS II is accurate, up-to-date and lawful.
2. Only the Member State issuing the alert shall be authorised to modify, add to, correct or delete data which it has entered.

3. If one of the Member States which has not issued the alert has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it shall advise the Member State issuing the alert thereof as soon as possible; the latter shall be obliged to check the communication and, if necessary, correct or delete the item in question immediately.
4. If the Member States are unable to reach agreement, the Member State which did not issue the alert shall submit the case to the joint supervisory authority referred to in Article 31 (3) for its opinion.
5. The Member States shall exchange supplementary information in order to distinguish accurately between alerts in the SIS II related to persons with similar characteristics.
6. Where a person is already the subject of an alert in the SIS II, 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.

Article 25

Additional data for the purpose of dealing with misidentifications of persons[16]

1. 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.
2. The data related to a person whose identity has been misused shall only be added with that person's explicit consent and shall only be used for the following purposes:

   to allow the competent authority to differentiate the person whose identity has been misused from the person actually intended by the alert;

   to allow the person whose identity has been misused to prove his identity and to establish that his identity has been misused.
3. No more than the following personal data may be entered and further processed in the SIS II for the purpose of this article:

   surname(s) and forename(s), any aliases possibly entered separately;

   any specific objective and physical characteristic not subject to change;

   date and place of birth;

[16] BE suggested the insertion of other biometric data than photographs and fingerprints.

sex;

photographs;

fingerprints;

nationality;

number(s) of identity paper(s) 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 may do so for the sole purpose of avoiding misidentification.

Article 26

Links between alerts

1. Subject to any restriction imposed by national legislation, a Member State may create a link between alerts it issues in the SIS II. The effect of such a link shall be to establish a relationship between two or more 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 conservation period of each of the linked alerts.

3. The creation of a link shall not affect the rights to access provided for in this Regulation. 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 there can be no access to the link from its national territory.

Article 27

Purpose and conservation period of supplementary information

1. Member States shall keep a copy of the decisions referred to in Article 14 A (2)(m) to support the exchange of supplementary information.

2. Personal data held in files by the authorities referred to in Article 7 (2) as a result of information exchanged pursuant to that paragraph, 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 alert related to the person concerned has been deleted from the SIS II.
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 of time for which such data may be held in such files shall be governed by national law.

CHAPTER VI
Data protection

Article 28
Right of information

1. The right of persons to have access to data entered in the SIS II in accordance with this Regulation which relate to them shall be exercised in accordance with the law of the Member State before which they invoke that right. If national law so provides, the national supervisory authority provided for in Article 31 (1) shall decide whether information shall be communicated and by what procedures. A Member State which has not issued the alert may communicate information concerning such data only if it has previously given the Member State issuing the alert an opportunity to state its position.
2. Communication of information to the data subject shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of the rights and freedoms of third parties.
3. Any person may have factually inaccurate data relating to them corrected or unlawfully stored data relating to them deleted.

Article 29

(...)

Article 30

Remedies

1. Any person may, in the territory of each Member State, bring before the courts or the authority competent under national law an action to correct, delete or obtain information or to obtain compensation in connection with an alert involving them.
2. The Member States undertake mutually to enforce final decisions taken by the courts or authorities referred to in paragraph 1, without prejudice to the provisions of Article 32.

Article 31

Data protection authorities

1. Each Member State shall designate a supervisory authority responsible in accordance with national law for carrying out independent supervision of the NS-SIS and for checking that the processing and use of data entered in the SIS II does not violate the rights of the data subject. For this purpose, where relevant, the supervisory authority shall have access to the national copy of the NS-SIS.
2. Any person shall have the right to ask the supervisory authorities to check data entered in the SIS II which concern them and the use made of such data. That right shall be governed by the national law of the Member State to which the request is made. If the data have been entered by another Member State, the check shall be carried out in close coordination with that Member State's supervisory authority.

3. A joint supervisory authority shall be set up and shall be responsible for supervising the CS-SIS. This authority shall consist of two representatives from each national supervisory authority. Each Member State shall have one vote. Supervision shall be carried out in accordance with the provisions of this Regulation, [the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector,].[17]

4. As regards the CS-SIS, the joint supervisory authority shall have the task of checking that the provisions of this Convention are properly implemented. For that purpose, it shall have access to the reference database for SIS II.

5. The joint supervisory authority shall also be responsible for examining any difficulties of application or interpretation that may arise during the operation of the SIS II, for studying any problems that may occur with the exercise of independent supervision by the national supervisory authorities of the Member States or in the exercise of the right of access to the system, and for drawing up harmonised proposals for joint solutions to existing problems.

6. Reports drawn up by the joint supervisory authority shall be submitted to the authorities to which the national supervisory authorities submit their reports and to the European Parliament.

[17] Delegates must consider the importance and role of Directive 95/46 and Regulation 45/2001. The Legal Service has doubts as to whether the EDPS can be sidelined entirely under the 1st pillar.

CHAPTER VII

Liability and sanctions

Article 32

Liability

1. Each Member State shall be liable in accordance with its national law for any injury caused to a person through the use of the NS-SIS. This shall also apply to injury caused by the Member State which issued the alert, where the latter entered factually inaccurate data or stored data unlawfully.
2. If 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 data were used by the requested Member State in breach of this Regulation.
3. If the failure of a Member State to comply with its obligations under this Regulation causes damage to the SIS II, that Member State shall be held liable for such damage, unless and insofar as the Management Authority or other Member State(s) participating in the SIS II failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.

Article 33

Sanctions

Member States shall ensure that any misuse of data entered into the SIS II is subject to effective, proportionate and dissuasive sanctions in accordance with national law.

CHAPTER VIII

Final Provisions

[The final provisions are closely connected to the political agreement on the management of SIS II and will therefore be discussed after a final decision.]